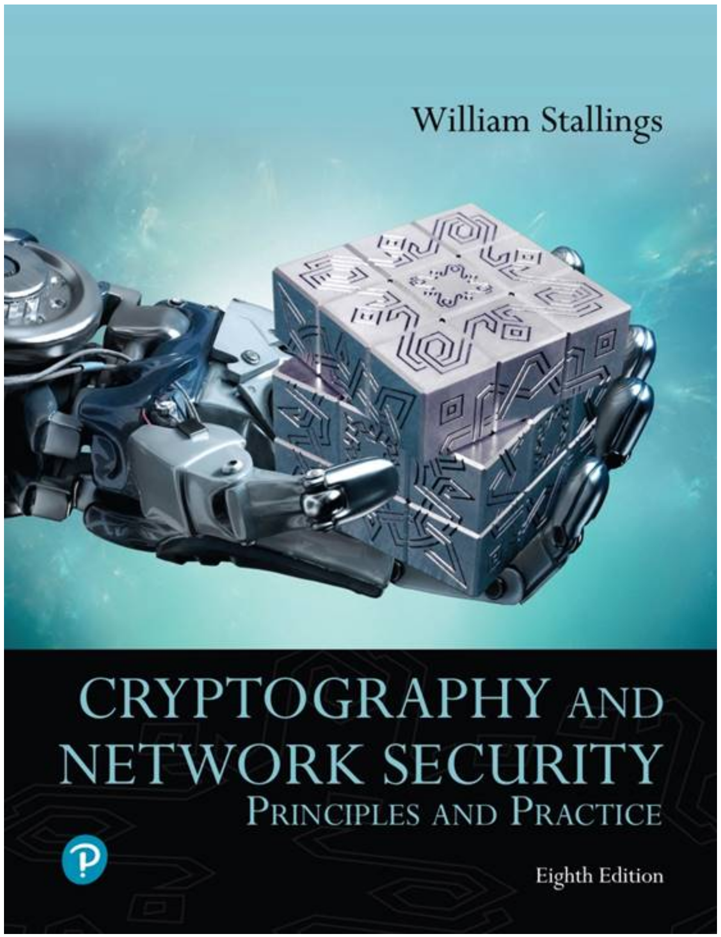
Cryptography and Network Security: Principles and Practice

Eighth Edition



Chapter 2

Introduction to Number Theory

Divisibility

- We say that a nonzero b **divides** a if $a = mb$ for some m, where a, b, and m are integers
- b divides a if there is no remainder on division
- The notation $b \mid a$ is commonly used to mean b divides a
- If $b \mid a$ we say that b is a **divisor** of a

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24

$13 \mid 182;\ -5 \mid 30;\ 17 \mid 289;\ -3 \mid 33;\ 17 \mid 0$

Properties of Divisibility (1 of 2)

- If $a \mid 1$, then $a = \pm 1$
- If $a \mid b$ and $b \mid a$, then $a = \pm b$
- Any $b \neq 0$ divides 0
- If $a \mid b$ and $b \mid c$, then $a \mid c$

$$\boxed{11 \mid 66 \text{ and } 66 \mid 198 \Rightarrow 11 \mid 198}$$

- If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$ for arbitrary integers m and n

2.1.4 Continued

Note

Fact 1: The integer 1 has only one divisor, itself.

Fact 2: Any positive integer has at least two divisors, 1 and itself (but it can have more).

Properties of Divisibility (2 of 2)

- To see this last point, note that:
  - If $b \mid g$, then g is of the form $g = b * g_1$ for some integer g_1
  - If $b \mid h$, then h is of the form $h = b * h_1$ for some integer h_1
- So:
  - $mg + nh = mbg_1 + nbh_1 = b * (mg_1 + nh_1)$

  and therefore b divides $mg + nh$

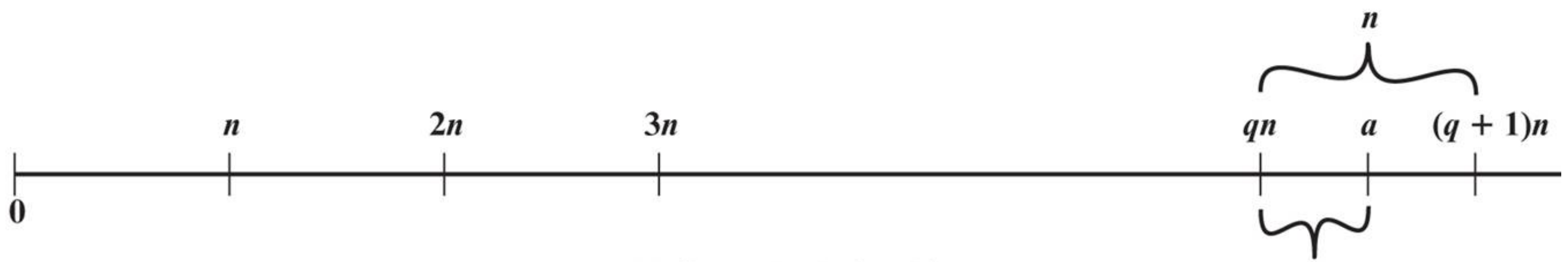
> $b = 7$; $g = 14$; $h = 63$; $m = 3$; $n = 2$
>
> 7 | 14 and 7 | 63.
>
> To show 7 (3 * 14 + 2 * 63),
>
> we have (3 * 14 + 2 * 63) = 7(3 * 2 + 2 * 9),
>
> and it is obvious that 7 | (7(3 * 2 + 2 * 9)).

Division Algorithm

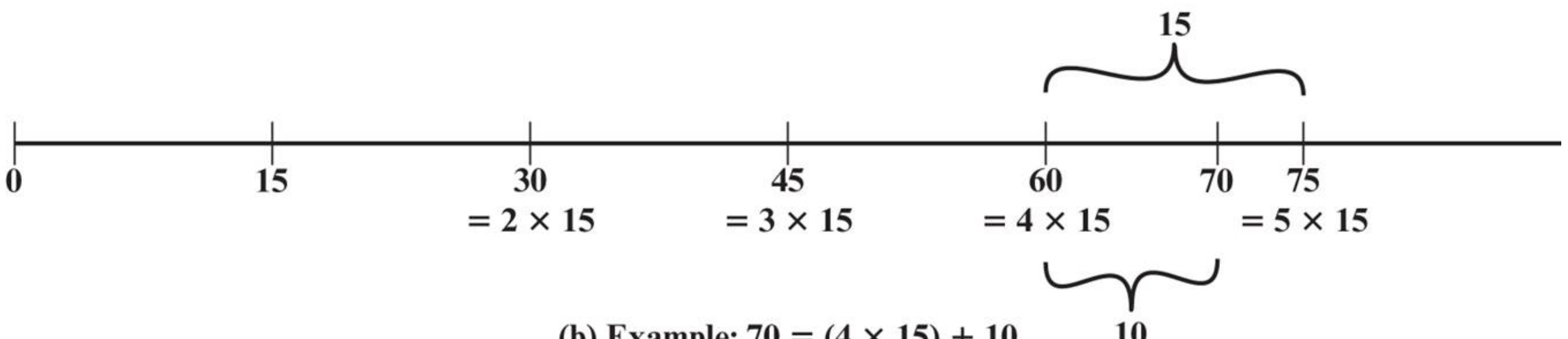
- Given any positive integer n and any nonnegative integer a, if we divide a by n we get an integer quotient q and an integer remainder r that obey the following relationship:

$$a = qn + r \qquad 0 \leq r < n;\ q = [a/n]$$

Figure 2.1 The Relationship $a = qn + r$; $0 \le r < n$



(a) General relationship



(b) Example: 70 = (4 × 15) + 10

Euclidean Algorithm

- One of the basic techniques of number theory
- Procedure for determining the greatest common divisor of two positive integers
- Two integers are **relatively prime** if their only common positive integer factor is 1

Greatest Common Divisor (GCD)

- The greatest common divisor of *a* and *b* is the largest integer that divides both *a* and *b*
- We can use the notation gcd(*a*,*b*) to mean the **greatest common divisor** of *a* and *b*
- We also define gcd(0,0) = 0
- Positive integer *c* is said to be the gcd of *a* and *b* if:
  - *c* is a divisor of *a* and *b*
  - Any divisor of *a* and *b* is a divisor of *c*
- An equivalent definition is:

$$\gcd(a,b) = \max[k, \text{ such that } k \mid a \text{ and } k \mid b]$$

GCD

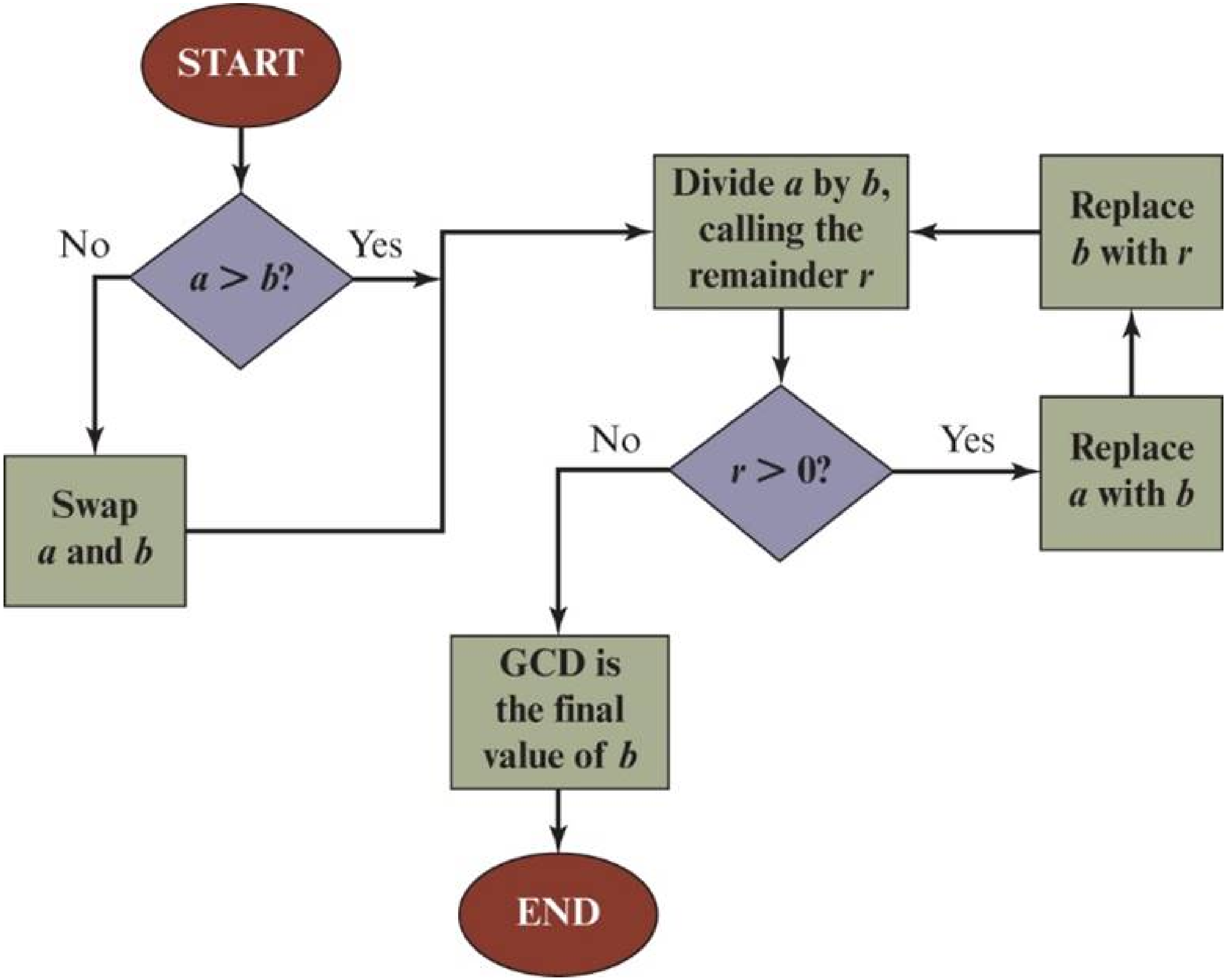
- Because we require that the greatest common divisor be positive, gcd(a,b) = gcd$(a, -b)$ = gcd$(-a,b)$ = gcd$(-a, -b)$
- In general, gcd(a,b) = gcd$(|a|, |b|)$

$$\boxed{\gcd(60, 24) = \gcd(60, -24) = 12}$$

- Also, because all nonzero integers divide 0, we have gcd(a,0) = | a |
- We stated that two integers a and b are relatively prime if their only common positive integer factor is 1; this is equivalent to saying that a and b are relatively prime if gcd$(a,b) = 1$

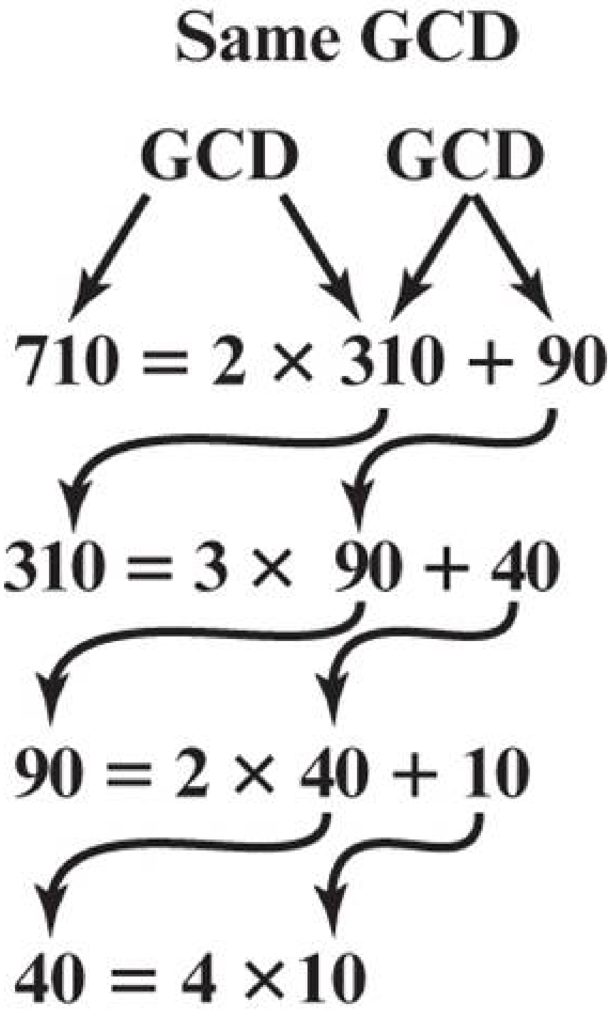
8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

Figure 2.2 Euclidean Algorithm



Pearson

Figure 2.3 Euclidean Algorithm Example: gcd(710, 310)



2.1.4 Continued

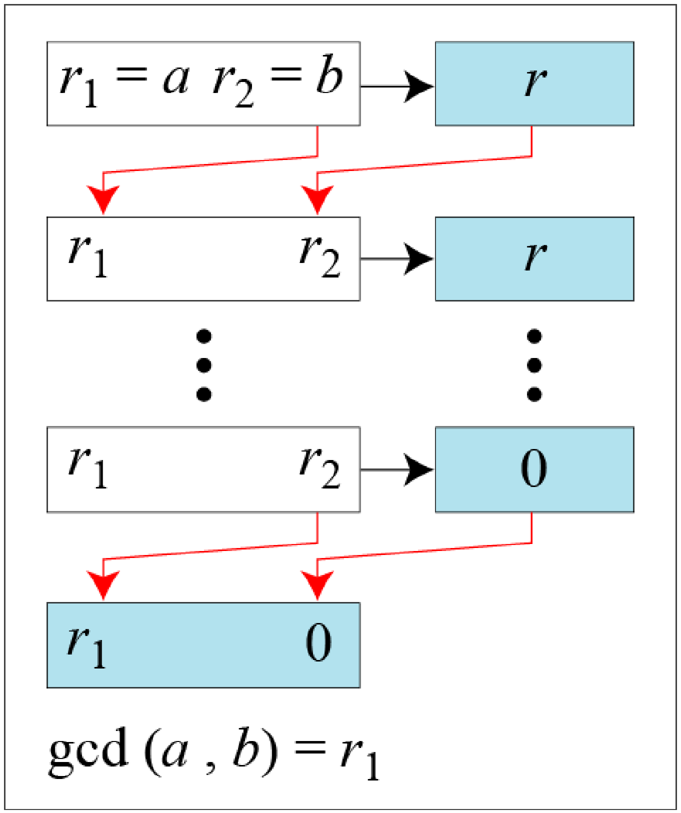
Note Greatest Common Divisor

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

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

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	

Find the greatest common divisor of 25 and 60.

Solution

We have gcd (25, 60) = 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	

Table 2.1 Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
$a = 1160718174$	$b = 316258250$	$q_1 = 3$	$r_1 = 211943424$
$b = 316258250$	$r_1 = 211943434$	$q_2 = 1$	$r_2 = 104314826$
$r_1 = 211943424$	$r_2 = 104314826$	$q_3 = 2$	$r_3 = 3313772$
$r_2 = 104314826$	$r_3 = 3313772$	$q_4 = 31$	$r_4 = 1587894$
$r_3 = 3313772$	$r_4 = 1587894$	$q_5 = 2$	$r_5 = 137984$
$r_4 = 1587894$	$r_5 = 137984$	$q_6 = 11$	$r_6 = 70070$
$r_5 = 137984$	$r_6 = 70070$	$q_7 = 1$	$r_7 = 67914$
$r_6 = 70070$	$r_7 = 67914$	$q_8 = 1$	$r_8 = 2156$
$r_7 = 67914$	$r_8 = 2156$	$q_9 = 31$	$r_9 = 1078$
$r_8 = 2156$	$r_9 = 1078$	$q_{10} = 2$	$r_{10} = 0$

Modular Arithmetic (1 of 3)

- The modulus
  - If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n; the integer n is called the **modulus**
  - Thus, for any integer a:

$$a = qn + r \quad 0 \le r < |n|; \quad q = [a/n]$$

$$a = [a/n] * n + (a \bmod n)$$

$$\boxed{11 \bmod 7 = 4; \; -11 \bmod 7 = 3}$$

Modular Arithmetic (2 of 3)

- Congruent modulo *n*
  - Two integers *a* and *b* are said to be **congruent modulo *n*** if (a mod n) = (b mod n)
  - This is written as $a \equiv b$ (mod n)
  - Note that if $a \equiv 0$ (mod n), then $n \mid a$

$$\boxed{73 \equiv 4 \pmod{23}; \quad 21 \equiv -9 \pmod{10}}$$

Properties of Congruences

- Congruences have the following properties:
  1. a ≡ b (mod n) if n | *(a – b)*
  2. a ≡ b (mod n) implies b ≡ a (mod n)
  3. a ≡ b (mod n) and b ≡ c (mod n) imply a ≡ c (mod n)

- To demonstrate the first point, if n | (a − b), then (a − b) = k*n for some *k*
  - So we can write a = b + *kn*
  - Therefore, *(a mod n)* = (remainder when b + *kn* is divided by n) = (remainder when *b* is divided by n) = (b mod n)

$$23 \equiv 8 \pmod 5 \text{ because } 23 - 8 = 15 = 5 * 3$$
$$-11 \equiv 5 \pmod 8 \text{ because } -11 - 5 = -16 = 8 * (-2)$$
$$81 \equiv 0 \pmod{27} \text{ because } 81 - 0 = 81 = 27 * 3$$

Modular Arithmetic (3 of 3)

- Modular arithmetic exhibits the following properties:
  1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  3. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$
- We demonstrate the first property:
  - Define $(a \bmod n) = r_a$ and $(b \bmod n) = r_b$. Then we can write $a = r_a + jn$ for some integer j and $b = r_b + kn$ for some integer k
  - Then:

$$
\begin{aligned}
(a + b) \bmod n &= (r_a + jn + r_b + kn) \bmod n \\
&= (r_a + r_b + (k + j)n) \bmod n \\
&= (r_a + r_b) \bmod n \\
&= [(a \bmod n) + (b \bmod n)] \bmod n
\end{aligned}
$$

Pearson

Remaining Properties

- Examples of the three remaining properties:

11 mod 8 = 3; 15 mod 8 = 7

[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2

(11 + 15) mod 8 = 26 mod 8 = 2

[(11 mod 8) − (15 mod 8)] mod 8 = − 4 mod 8 = 4

(11 − 15) mod 8 = − 4 mod 8 = 4

[(11 mod 8) * (15 mod 8)] mod 8 = 21 mod 8 = 5

(11 * 15) mod 8 = 165 mod 8 = 5

Table 2.2 (a) Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Table 2.2 (b) Multiplication Modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Table 2.2 (c) Additive and Multiplicative Inverse Modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

Table 2.3 Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse ($-w$)	For each $w \in Z_n$, there exists a z such that $w + z$ 0 mod n

2.1.4 Continued

Properties

***Property 1:** if $a|1$, then $a = \pm 1$.*

***Property 2:** if $a|b$ and $b|a$, then $a = \pm b$.*

***Property 3:** if $b|a$ and $c|b$, then $c|a$.*

***Property 4:** if $a|b$ and $a|c$, then $a|(m \times b + n \times c)$, where m and n are arbitrary integers*

Pearson

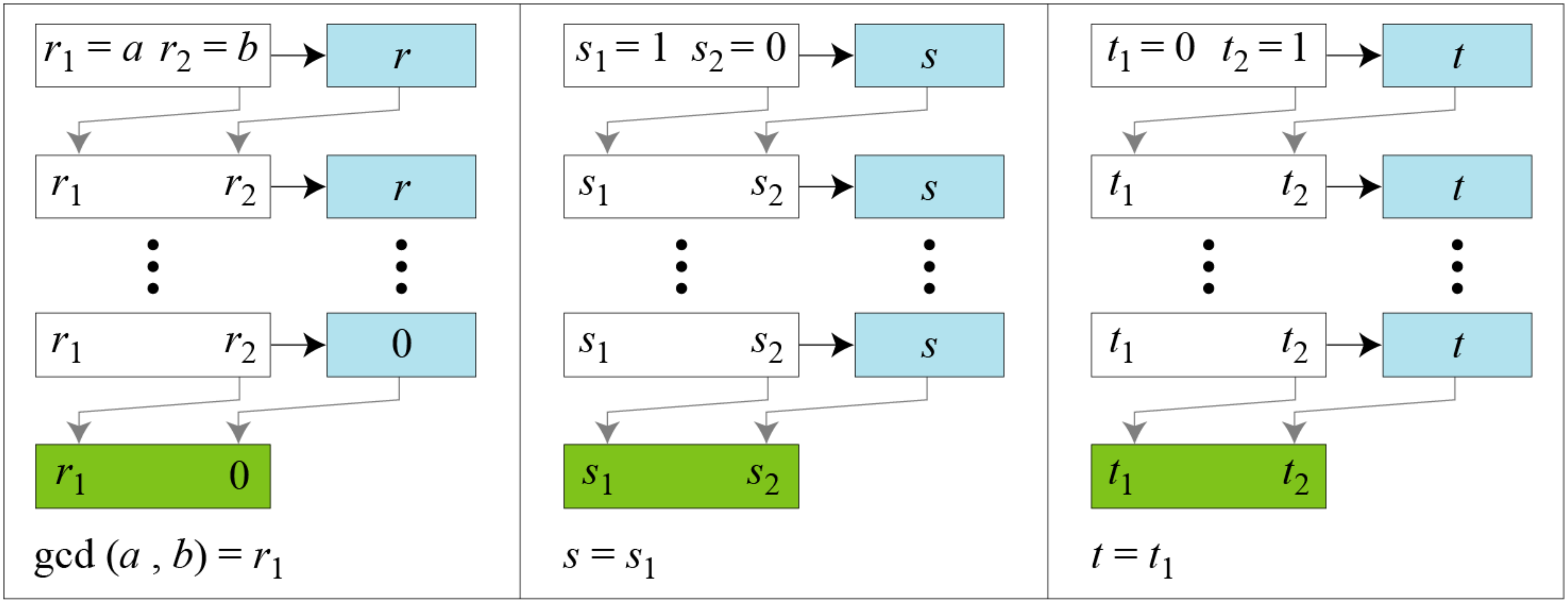
Extended Euclidean Algorithm

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, part a



a. Process

Extended Euclidean algorithm, part b

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

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

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

Example

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	

Example

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	

Example

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	

Additional: Running Extended Euclidean Algorithm Manually

Given *a* = 80 and *b* = 62, find gcd (*a*, *b*) and the values of *s* and *t*.

Solution

gcd(80,62) = s*(80) + t*(62) proceeds as:

	in equation form	in row form		
row1	80 = 1(80) + 0(62)	80	1	0
row2	62 = 0(80) + 1(62)	62	0	1
row1 – 1* row2	18 = 1(80) - 1(62)	18	1	-1
row2 – 3* row3	8 = -3(80) + 4(62)	8	-3	4
row3 – 2* row4	2 = 7(80) - 9(62)	2	7	-9
row4 – 4* row5	0 = -31(80) +40(62)	0	-31	40

gcd(80,62) = 2 = 7*(80) + (-9)*(62)

Table 2.4 Extended Euclidean Algorithm Example

i	r_i	q_i	x_i	y_i
−1	1759		1	0
0	550		0	1
1	109	3	1	−3
2	5	5	−5	16
3	4	21	106	−339
4	1	1	−111	355
5	0	4		

Result: $d = 1$; $x = -111$; $y = 355$

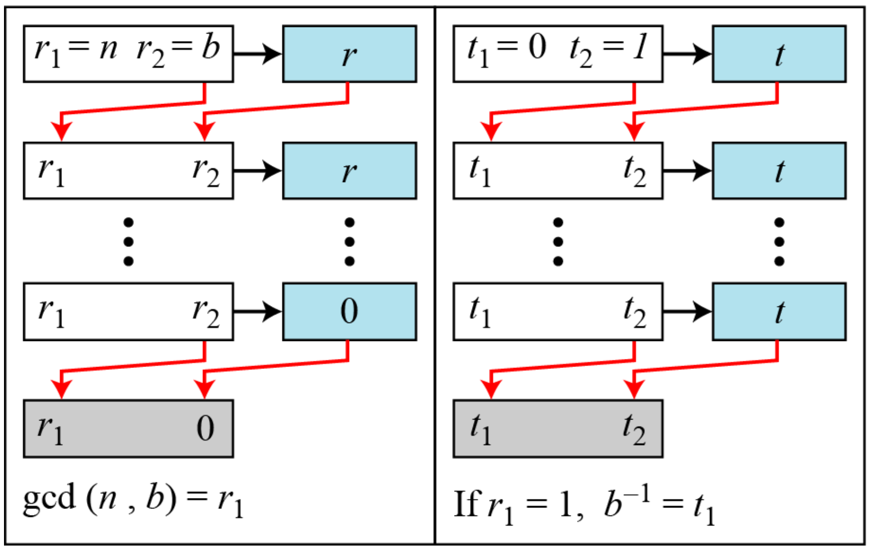
Multiplicative Inverses

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.

Continued

Figure 2.15 Using extended Euclidean algorithm to find multiplicative inverse



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

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.

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.

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.

Prime Numbers

- Prime numbers only have divisors of 1 and itself
  - They cannot be written as a product of other numbers
- Prime numbers are central to number theory
- Any integer $a > 1$ can be factored in a unique way as

$$a = p_1^{a_1} * p_2^{a_2} * \ldots * p_{pt}^{a_t}$$

where $p_1 < p_2 < \ldots < p_t$ are prime numbers and where each a_i is a positive integer

- This is known as the fundamental theorem of arithmetic

Pearson

Table 2.5 Primes Under 2000

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Summary

- Understand the concept of divisibility and the division algorithm
- Understand how to use the Euclidean algorithm to find the greatest common divisor
- Present an overview of the concepts of modular arithmetic
- Explain the operation of the extended Euclidean algorithm
- Discuss key concepts relating to prime numbers
- Understand Fermat's theorem
- Understand Euler's theorem
- Define Euler's totient function
- Make a presentation on the topic of testing for primality
- Explain the Chinese remainder theorem
- Define discrete logarithms

Copyright

This work is protected by United States copyright laws and is provided solely for the use of instructors in teaching their courses and assessing student learning. Dissemination or sale of any part of this work (including on the World Wide Web) will destroy the integrity of the work and is not permitted. The work and materials from it should never be made available to students except by instructors using the accompanying text in their classes. All recipients of this work are expected to abide by these restrictions and to honor the intended pedagogical purposes and the needs of other instructors who rely on these materials.