Chapter 4

Basic Concepts in Number Theory and Finite Fields

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

- 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 $a \mid c$

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

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

Properties of Divisibility

- 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 $mg + nh$

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

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:

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

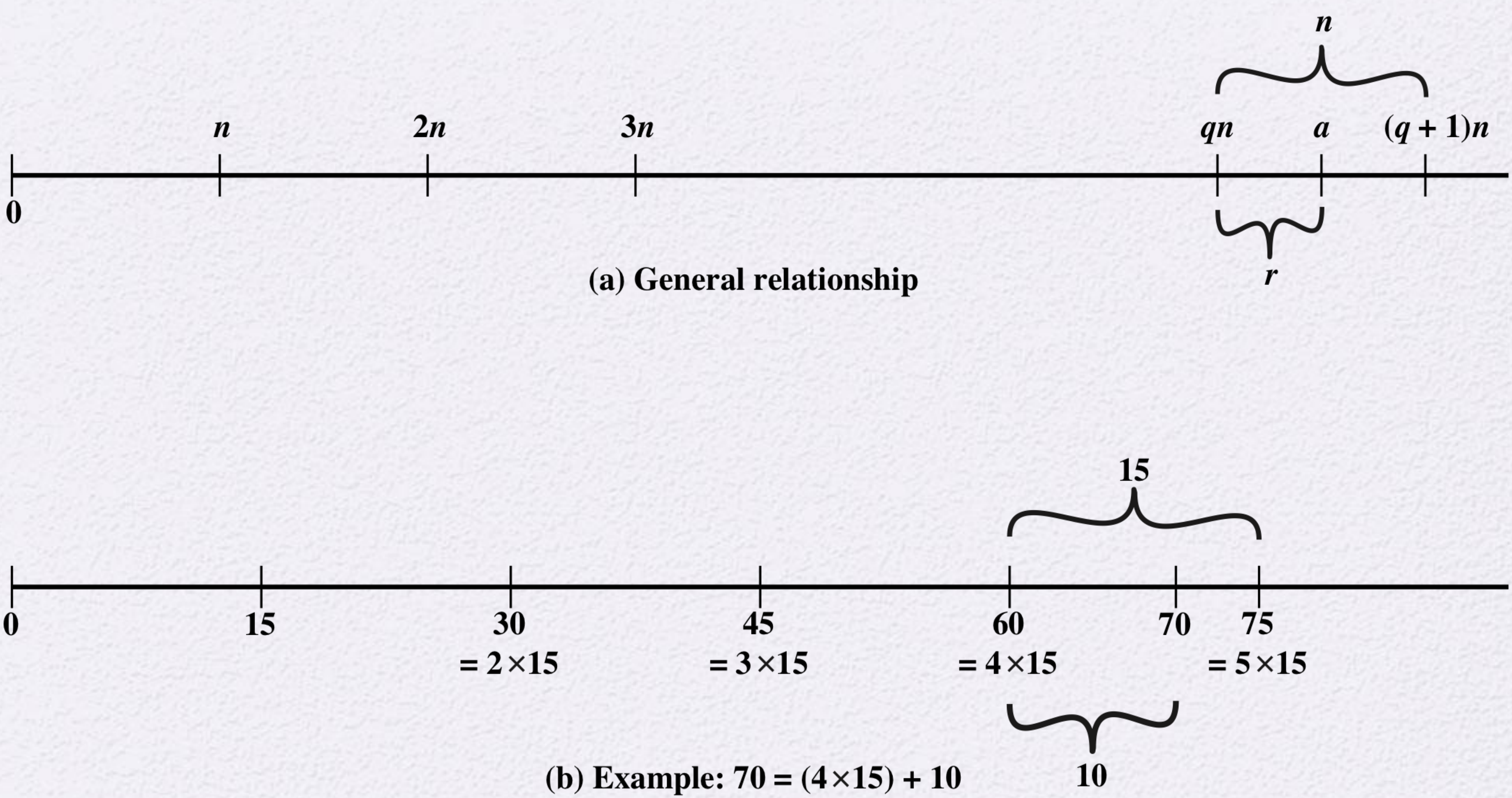

Figure 4.1 The Relationship $a = qn + r;\ 0 \le r < n$

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 |)

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.

GCD

- Euclid algorithm for easily finding the greatest common divisor of two integers.

- Suppose we have integers a, b such that d = gcd(a, b).
  - Now dividing a by b and applying the division algorithm

$$a = q_1 b + r_1 \qquad 0 \le r_1 < b$$

$$b = q_2 r_1 + r_2 \qquad 0 \le r_2 < r_1$$

$$\left.\begin{array}{ll} a = q_1 b + r_1 & 0 < r_1 < b \\ b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\ \quad\vdots & \quad\vdots \\ r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = q_{n+1} r_n + 0 & \\ d = \gcd(a, b) = r_n & \end{array}\right\}$$

Euclidean Algorithm Example

To find $d = \gcd(a,b) = \gcd(1160718174, 316258250)$		
$a = q_1 b + r_1$	$1160718174 = 3 \times 316258250 + 211943424$	$d = \gcd(316258250, 211943424)$
$b = q_2 r_1 + r_2$	$316258250 = 1 \times 211943424 + 104314826$	$d = \gcd(211943424, 104314826)$
$r_1 = q_3 r_2 + r_3$	$211943424 = 2 \times 104314826 + 3313772$	$d = \gcd(104314826, 3313772)$
$r_2 = q_4 r_3 + r_4$	$104314826 = 31 \times 3313772 + 1587894$	$d = \gcd(3313772, 1587894)$
$r_3 = q_5 r_4 + r_5$	$3313772 = 2 \times 1587894 + 137984$	$d = \gcd(1587894, 137984)$
$r_4 = q_6 r_5 + r_6$	$1587894 = 11 \times 137984 + 70070$	$d = \gcd(137984, 70070)$
$r_5 = q_7 r_6 + r_7$	$137984 = 1 \times 70070 + 67914$	$d = \gcd(70070, 67914)$
$r_6 = q_8 r_7 + r_8$	$70070 = 1 \times 67914 + 2156$	$d = \gcd(67914, 2156)$
$r_7 = q_9 r_8 + r_9$	$67914 = 31 \times 2516 + 1078$	$d = \gcd(2156, 1078)$
$r_8 = q_{10} r_9 + r_{10}$	$2156 = 2 \times 1078 + 0$	$d = \gcd(1078, 0) = 1078$
Therefore, $d = \gcd(1160718174, 316258250) = 1078$		

Table 4.1
Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
$a =$ 1160718174	$b =$ 316258250	$q_1 =$ 3	$r_1 =$ 211943424
$b =$ 316258250	$r_1 =$ 211943424	$q_2 =$ 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

(This table can be found on page 91 in the textbook)

Modular Arithmetic

- 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*:

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

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

11 mod 7 = 4; - 11 mod 7 = 3

Modular Arithmetic

- 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 $a = b$(mod n)
  - Note that if $a = 0$(mod n), then $n \mid a$

73 = 4 (mod 23);   21 = - 9 (mod 10)

Properties of Congruences

- Congruences have the following properties:

    1. $a = b \pmod{n}$ if $n \mid (a - b)$

    2. $a = b \pmod{n}$ implies $b = a \pmod{n}$

    3. $a = b \pmod{n}$ and $b = c \pmod{n}$ imply $a = c \pmod{n}$

- To demonstrate the first point, if $n|(a - b)$, then $(a - b) = kn$ 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 = 8 (mod 5) because 23 - 8 = 15 = 5 * 3
- 11 = 5 (mod 8) because - 11 - 5 = - 16 = 8 * (- 2)
81 = 0 (mod 27) because 81 - 0 = 81 = 27 * 3

Modular Arithmetic

- 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. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

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 4.2(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 4.2(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 4.2(c)

Additive and Multiplicative Inverses 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 4.3

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 $w + z \equiv 0 \bmod n$

Extended Euclidean Algorithm Example

x / *y*	**−3**	**−2**	**−1**	**0**	**1**	**2**	**3**
−3	−216	−174	−132	−90	−48	−6	36
−2	−186	−144	−102	−60	−18	24	66
−1	−156	−114	−72	−30	12	54	96
0	−126	−84	−42	0	42	84	126
1	−96	−54	−12	30	72	114	156
2	−66	−24	18	60	102	144	186
3	−36	6	48	90	132	174	216

Table 4.4
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

Summary

- Divisibility and the division algorithm
- The Euclidean algorithm
- Modular arithmetic
- Groups, rings, and fields

- Finite fields of the form GF(p)
- Polynomial arithmetic
- Finite fields of the form GF(2^n)