Chapter 2 Introduction To Number Theory

"Mathematics has long been known in the printing trade as difficult, or penalty, copy because it is slower, more difficult, and more expensive to set in type than any other kind of copy."

—Chicago Manual of Style,
14th Edition

Outline

- Divisibility and The Division Algorithm
- The Euclidean Algorithm
- Modular Arithmetic
- Prime Numbers
- Fermat’s and Euler’s Theorems
- Testing for Primality
- The Chinese Remainder Theorem
- Discrete Logarithms

Outline

- Divisibility and The Division Algorithm
- The Euclidean Algorithm
- Modular Arithmetic
- Prime Numbers
- Fermat’s and Euler’s Theorems
- Testing for Primality
- The Chinese Remainder Theorem
- Discrete Logarithms

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* | *a* is commonly used to mean *b* divides *a***
- **If *b* | *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 | 182; - 5 | 30; 17 | 289; - 3 | 33; 17 | 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 $a \mid c$

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

- 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 | 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:**

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

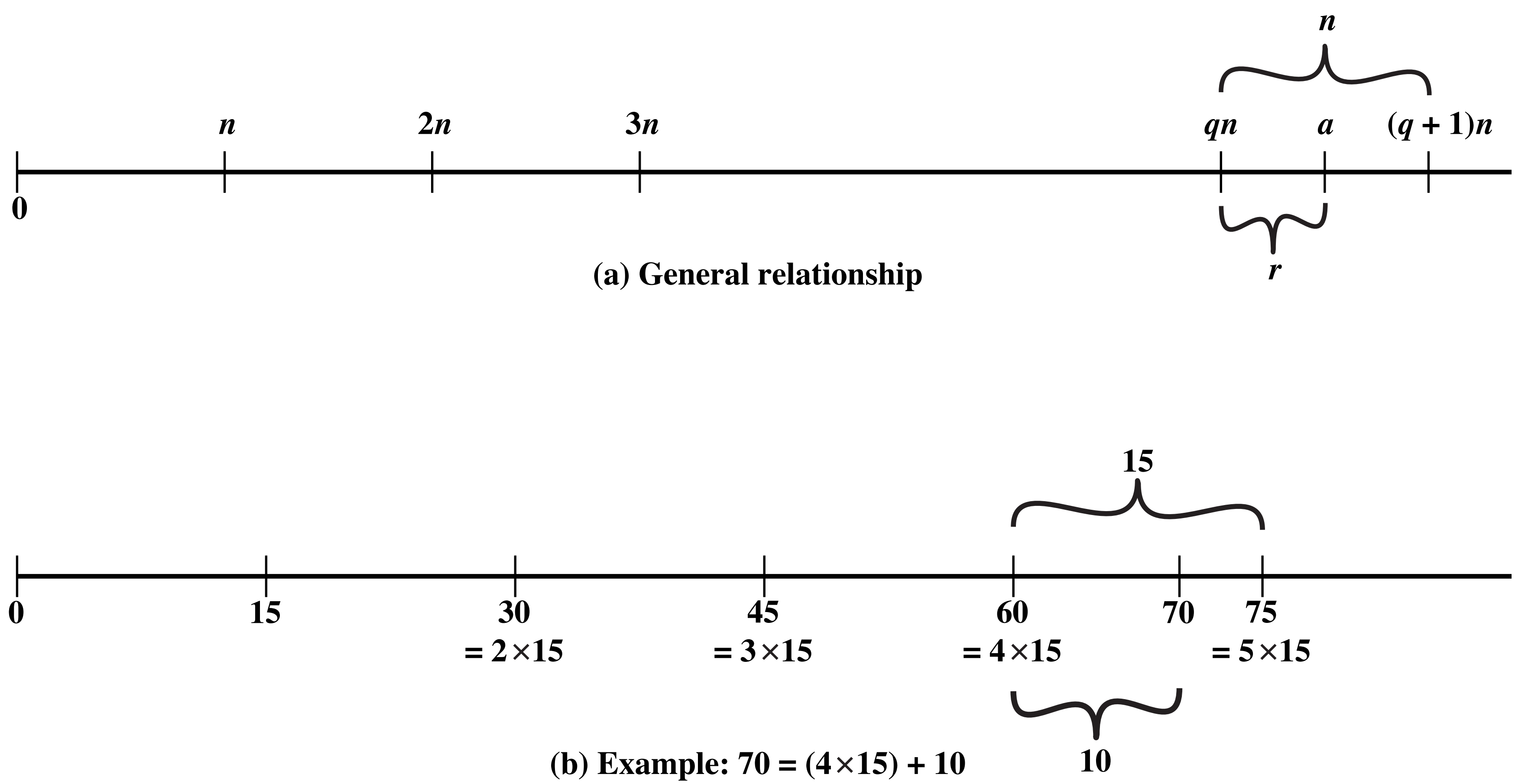


Figure 2.1 The Relationship $a = qn + r;\ 0 \le r < n$

Residue

- **Given a and positive n, it is always possible to find q and r that satisfy the preceding relationship**
  - Represent the integers on the number line
  - a will fall somewhere on that line (positive a is shown, a similar demonstration can be made for negative a)
    - Starting at 0, proceed to n, 2n, up to qn, such that qn<=a and (q+1)n>a
  - The distance from qn to a is r, and we have found the unique values of q and r
  - The remainder r is often referred to as a residue

$a = 11;$	$n = 7;$	$11 = 1 \times 7 + 4;$	$r = 4$	$q = 1$
$a = -11;$	$n = 7;$	$-11 = (-2) \times 7 + 3;$	$r = 3$	$q = -2$

Figure 2.1b provides another example.

Outline

- ❑ Divisibility and The Division Algorithm
- ❑ **The Euclidean Algorithm**
- ❑ Modular Arithmetic
- ❑ Prime Numbers
- ❑ Fermat's and Euler's Theorems
- ❑ Testing for Primality
- ❑ The Chinese Remainder Theorem
- ❑ Discrete Logarithms

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.

Greatest Common Divisor (GCD)

- **a common problem in number theory**
- **GCD (a,b) of a and b is the largest number that divides evenly into both a and b**
  - eg GCD(60,24) = 12
- **often want no common factors (except 1) and hence numbers are relatively prime**
  - eg GCD(8,15) = 1
  - hence 8 & 15 are relatively prime

Euclidean Algorithm

1. Suppose we wish to determine the greatest common divisor d of the integers a and b; that is determine $d = \gcd(a, b)$. Because $\gcd(|a|, |b|) = \gcd(a, b)$, there is no harm in assuming $a \geq b > 0$.
2. Dividing a by b and applying the division algorithm, we can state:

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b \tag{2.2}$$

3. First consider the case in which $r_1 = 0$. Therefore b divides a and clearly no larger number divides both b and a, because that number would be larger than b. So we have $d = \gcd(a, b) = b$.
4. The other possibility from Equation (2.2) is $r_1 \neq 0$. For this case, we can state that $d|r_1$. This is due to the basic properties of divisibility: the relations $d|a$ and $d|b$ together imply that $d|(a - q_1 b)$, which is the same as $d|r_1$.
5. Before proceeding with the Euclidian algorithm, we need to answer the question: What is the $\gcd(b, r_1)$? We know that $d|b$ and $d|r_1$. Now take any arbitrary integer c that divides both b and r_1. Therefore, $c|(q_1 b + r_1) = a$. Because c divides both a and b, we must have $c \leq d$, which is the greatest common divisor of a and b. Therefore $d = \gcd(b, r_1)$.

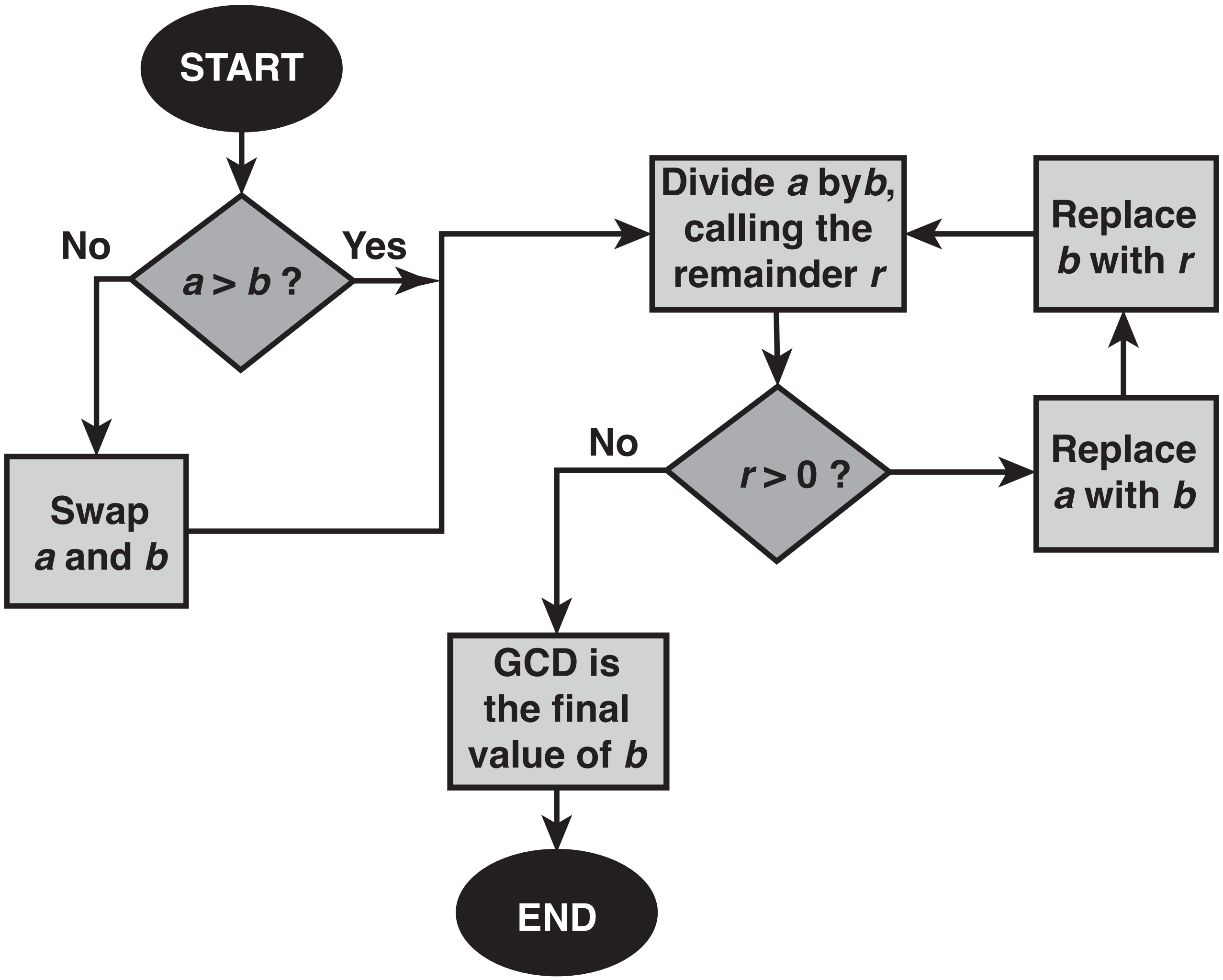


Figure 2.2 Euclidean Algorithm

Finding The GCD

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

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

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

Same GCD

GCD GCD

$$710 = 2 \times 310 + 90$$

$$310 = 3 \times 90 + 40$$

$$90 = 2 \times 40 + 10$$

$$40 = 4 \times 10$$

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

Example GCD(1970,1066)

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	gcd(2, 0)

Example of GCD

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, $d = \gcd(1160718174, 316258250) = 1078$		

Example of GCD

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

Outline

- Divisibility and The Division Algorithm
- The Euclidean Algorithm
- Modular Arithmetic
- Prime Numbers
- Fermat's and Euler's Theorems
- Testing for Primality
- The Chinese Remainder Theorem
- Discrete Logarithms

Modular Arithmetic

- **define modulo operator `a mod n` to be remainder when a is divided by n**
- **use the term congruence for: $a \equiv b \bmod n$**
  - when divided by *n,* a & b have same remainder
  - eg. $100 \equiv 34 \bmod 11$
- **b is called the residue of a mod n**
  - since with integers can always write: `a = qn + b`
- **usually have `0 <= b <= n-1`**

  $-12 \bmod 7 \equiv -5 \bmod 7 \equiv 2 \bmod 7 \equiv 9 \bmod 7$

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

Modulo Operator

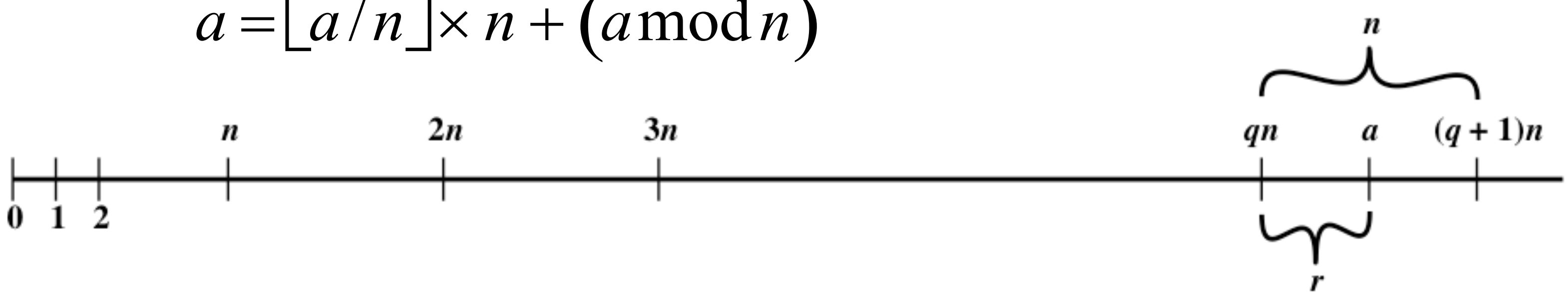
Given: positive integer n, any integer a

Then: divide a by n --> get quotient q and remainder (residue) r

$$a = qn + r \qquad 0 \le r < n\,;\, q = \lfloor a / n \rfloor$$

with modulo operator:

$$a = \lfloor a / n \rfloor \times n + (a \bmod n)$$



Set of residues Z_n={0,1,..,(n-1)}

"a and b congruent modulo n" if (a mod n) = (b mod n)

$$a \equiv b \bmod n$$

Modulo 7 Example

```
...
-21 -20 -19 -18 -17 -16 -15
-14 -13 -12 -11 -10  -9  -8
 -7  -6  -5  -4  -3  -2  -1
  0   1   2   3   4   5   6
  7   8   9  10  11  12  13
 14  15  16  17  18  19  20
 21  22  23  24  25  26  27
 28  29  30  31  32  33  34
...
```

Divisors

"b divides a" if there is no remainder on division --> $b|a$

- If $a|1$, then $a = \pm 1$
- If $a|b$ and $b|a$, then $a = \pm b$
- Any $b \neq 0$ divides 0
- If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n

- eg. all of 1,2,3,4,6,8,12,24 divide 24

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)

Modular Arithmetic Operations

- is 'clock arithmetic'
- uses a finite number of values, and loops back from either end
- modular arithmetic is when do addition & multiplication and modulo reduce answer
- can do reduction at any point, ie
  - a+b mod n = [a mod n + b mod n] mod n

Modulo Properties

Following properties hold:

$$a \equiv b \bmod n \quad \text{if } \; \mathrm{n} \,|\, (\mathrm{a} - \mathrm{b})$$

$$a \equiv b \bmod n \quad \text{implies} \quad b \equiv a \bmod n$$

$$a \equiv b \bmod n \quad \text{and} \quad b \equiv c \bmod n \quad \text{imply} \quad a \equiv c \bmod n$$

Modulo Arithmetic:

$$\left[(a \bmod n) + (b \bmod n)\right] \bmod n = (a + b) \bmod n$$

$$\left[(a \bmod n) - (b \bmod n)\right] \bmod n = (a - b) \bmod n$$

$$\left[(a \bmod n) \times (b \bmod n)\right] \bmod n = (a \times b) \bmod n$$

Properties of Congruences

- **Congruences have the following properties:**
  1. $a = b \pmod{n}$ if $n|(a - b)$
  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. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$
- **can do reduction at any point**
- **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:

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

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

Modular Arithmetic for modulo 8

Addition 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

Modular Arithmetic for modulo 8

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

Modular Arithmetic for modulo 8

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

w has multiplicative inverse iff *w* is relative prime to *n*

Properties of Modular Arithmetic

Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{0, 1, \ldots, (n - 1)\}$$

This is referred to as the **set of residues**, or **residue classes** (mod n).

$$[r] = \{a\colon a \text{ is an integer}, a \equiv r \pmod{n}\}$$

The residue classes (mod 4) are

$$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$$
$$[1] = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$$
$$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$$
$$[3] = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$$

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 $w + z \equiv 0 \bmod n$

Modular Arithmetic

- **can do modular arithmetic with any group of integers: $Z_n = \{0, 1, \ldots, n-1\}$**
- **form a commutative ring for addition (will be discussed later)**
- **with a multiplicative identity**
- **note some peculiarities**
  - if $(a+b) \equiv (a+c) \bmod n$ then $b \equiv c \bmod n$
  - but $(ab) \equiv (ac) \bmod n$ then $b \equiv c \bmod n$ only if a is relatively prime to n

Relatively Prime

- Another peculiarity:
  - $(ab) \equiv (ac) \bmod n$ then $b \equiv c \bmod n$ only if a is relatively prime to n

- Two integers are relatively prime if their only common positive integer factor is 1

$$((a^{-1})ab) \equiv ((a^{-1})ac)(\bmod n)$$
$$b \equiv c(\bmod n)$$

To see this, consider an example in which the condition of Equation (4.5) does not hold. The integers 6 and 8 are not relatively prime, since they have the common factor 2. We have the following:

$$6 \times 3 = 18 \equiv 2(\bmod 8)$$
$$6 \times 7 = 42 \equiv 2(\bmod 8)$$

Yet $3 \not\equiv 7 \ (\bmod 8)$.

Multiplicative Inverse

- An integer has a multiplicative inverse in Z_n if that integer is relatively prime to n

With $a = 6$ and $n = 8$,

Z_8	0	1	2	3	4	5	6	7
Multiply by 6	0	6	12	18	24	30	36	42
Residues	0	6	4	2	0	6	4	2

Because we do not have a complete set of residues when multiplying by 6, more than one integer in Z_8 maps into the same residue. Specifically, $6 \times 0 \bmod 8 = 6 \times 4 \bmod 8$; $6 \times 1 \bmod 8 = 6 \times 5 \bmod 8$; and so on. Because this is a many-to-one mapping, there is not a unique inverse to the multiply operation.

However, if we take $a = 5$ and $n = 8$, whose only common factor is 1,

Z_8	0	1	2	3	4	5	6	7
Multiply by 5	0	5	10	15	20	25	30	35
Residues	0	5	2	7	4	1	6	3

The line of residues contains all the integers in Z_8, in a different order.

Euclidean Algorithm Revisited

- **For any integers a, b with a>=b>=0:**

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

$$\gcd(55, 22) = \gcd(22, 55 \bmod 22) = \gcd(22, 11) = 11$$

- **Used repetitively to determine the greatest common divisor:**

$$\gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$$
$$\gcd(11, 10) = \gcd(10, 1) = \gcd(1, 0) = 1$$

Euclid's Algorithm

Integer *c* is greatest common divisor *gcd(a,b)* of *a* and *b* if

1. *c* is a divisor of *a* and of *b*
2. any divisor of *a* and *b* is a divisor of *c*

gcd(a,b) = gcd(b, a mod b)

```
Euclid(a,b)
    if (b=0) then return a;
    else return Euclid(b, a mod b);
```

Euclidean Algorithm

Euclidean Algorithm	
Calculate	**Which satisfies**
$r_1 = a \bmod b$	$a = q_1 b + r_1$
$r_2 = b \bmod r_1$	$b = q_2 r_1 + r_2$
$r_3 = r_1 \bmod r_2$	$r_1 = q_3 r_2 + r_3$
• • •	• • •
$r_n = r_{n-2} \bmod r_{n-1}$	$r_{n-2} = q_n r_{n-1} + r_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$	$r_{n-1} = q_{n+1} r_n + 0$ $d = \gcd(a, b) = r_n$

Euclidean Algorithm

- **Proof: gcd(a, b) = gcd(b, a mod b)**

Let d = gcd(a, b), then d|a and d|b

a = kb + r ≡ r (mod b)

a mod b = r

(a mod b) = a – kb

Since d|b and d|a, then d|(a mod b)

d is a common divisor of b and (a mod b)

If d is a common divisor of b and (a mod b),

then d|kb, d|[kb+(a mod b)], so d|a

Thus, the set of common divisor of a and b is equal to the set of common divisors of b and (a mod b)

Extended Euclidean Algorithm

$$ax + by = d = \gcd(a, b)$$

a = 42 and b = 30

gcd(42, 30) = 6

Table for 42x + 30y :

y \ x	–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

Proof 1

- The proof that follows may be adapted for any Euclidean domain.
- For given nonzero integers a and b there is a nonzero integer $d = as + bt$ of **minimal absolute value** among all those of the form $ax + by$ with x and y integers; one can assume $d > 0$ by changing the signs of both s and t if necessary.
- Now the remainder of dividing either a or b by d is also of the form $ax + by$ since it is obtained by subtracting a multiple of $d = as + bt$ from a or b, and on the other hand it has to be strictly smaller in absolute value than d. This leaves 0 as only possibility for such a remainder, so d divides a and b exactly.
- If c is another common divisor of a and b, then c also divides $as + bt = d$. Since c divides d but is not equal to it, it must be less than d. This means that d is the greatest common divisor of a and b;
- this completes the proof

Proof 2

For any pair of positive integers a and b, there exist $x, y \in \mathbb{Z}$ so that $ax + by = \gcd(a, b)$.

Proof:

Consider the set

$$K = \{ax + by \mid x, y \in \mathbb{Z}\} \tag{1}$$

Let k be the smallest positive element of K. Since $k \in K$, there are $x, y \in \mathbb{Z}$ so that

$$k = ax + by \tag{2}$$

Because $\mathbb{Z}$ is a Euclidean Domain, we can write

$$a = qk + r \text{ with } 0 \le r < k \tag{3}$$

Therefore, we can write

$$\begin{aligned} r &= a - qk \\ &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy) \\ &\in K \end{aligned} \tag{4}$$

Since k is the smallest *positive* element in K, (3) and (4) imply that r must be 0. Thus, $a = qk$, and therefore, k divides a. Similarly, k divides b. Thus, k is a common divisor of a and b, and therefore, $k \le \gcd(a, b)$.

Since $\gcd(a, b)$ divides both a and b, and $k = ax + by$, $\gcd(a, b)$ divides k.

Since $\gcd(a, b)$ divides k and $k \le \gcd(a, b)$, we get that $k = \gcd(a, b)$. Thus, (2) becomes

$$\gcd(a, b) = ax + by \tag{5}$$

Extended Euclidean Algorithm

$$r_i = ax_i + by_i$$

$$\begin{array}{ll} a = q_1 b + r_1 & r_1 = ax_1 + by_1 \\ b = q_2 r_1 + r_2 & r_2 = ax_2 + by_2 \\ r_1 = q_3 r_2 + r_3 & r_3 = ax_3 + by_3 \\ \vdots & \vdots \\ r_{n-2} = q_n r_{n-1} + r_n & r_n = ax_n + by_n \\ r_{n-1} = q_{n+1} r_n + 0 & \end{array}$$

$$r_i = r_{i-2} - r_{i-1} q_i$$

$$r_{i-2} = ax_{i-2} + by_{i-2} \quad \text{and} \quad r_{i-1} = ax_{i-1} + by_{i-1}$$

$$\begin{aligned} r_i &= (ax_{i-2} + by_{i-2}) - (ax_{i-1} + by_{i-1})q_i \\ &= a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) \end{aligned}$$

$$x_i = x_{i-2} - q_i x_{i-1} \quad \text{and} \quad y_i = y_{i-2} - q_i y_{i-1}$$

Extended Euclidean Algorithm

Extended Euclidean Algorithm			
Calculate	**Which satisfies**	**Calculate**	**Which satisfies**
$r_{-1} = a$		$x_{-1} = 1; y_{-1} = 0$	$a = ax_{-1} + by_{-1}$
$r_0 = b$		$x_0 = 0; y_0 = 1$	$b = ax_0 + by_0$
$r_1 = a \bmod b$ $q_1 = \lfloor a/b \rfloor$	$a = q_1 b + r_1$	$x_1 = x_{-1} - q_1 x_0 = 1$ $y_1 = y_{-1} - q_1 y_0 = -q_1$	$r_1 = ax_1 + by_1$
$r_2 = b \bmod r_1$ $q_2 = \lfloor b/r_1 \rfloor$	$b = q_2 r_1 + r_2$	$x_2 = x_0 - q_2 x_1$ $y_2 = y_0 - q_2 y_1$	$r_2 = ax_2 + by_2$
$r_3 = r_1 \bmod r_2$ $q_3 = \lfloor r_1/r_2 \rfloor$	$r_1 = q_3 r_2 + r_3$	$x_3 = x_1 - q_3 x_2$ $y_3 = y_1 - q_3 y_2$	$r_3 = ax_3 + by_3$
• • •	• • •	• • •	• • •
$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \lfloor r_{n-2}/r_{n-3} \rfloor$	$r_{n-2} = q_n r_{n-1} + r_n$	$x_n = x_{n-2} - q_n x_{n-1}$ $y_n = y_{n-2} - q_n y_{n-1}$	$r_n = ax_n + by_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \lfloor r_{n-1}/r_{n-2} \rfloor$	$r_{n-1} = q_{n+1} r_n + 0$		$d = \gcd(a, b) = r_n$ $x = x_n; y = y_n$

Extended Euclidean Algorithm Example

- a = 1759 and b = 550
- 1759x + 550y = gcd(1759, 550)
- 1759x(-111) + 550x355 = -195249 + 195250 = 1

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

Extended Euclidean Algorithm for Multiplicative Inverse

$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \lfloor r_{n-2}/r_{n-3} \rfloor$	$r_{n-2} = q_n r_{n-1} + r_n$	$x_n = x_{n-2} - q_n x_{n-1}$ $y_n = y_{n-2} - q_n y_{n-1}$	$r_n = ax_n + by_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \lfloor r_{n-1}/r_{n-2} \rfloor$	$r_{n-1} = q_{n+1} r_n + 0$		$d = \gcd(a, b) = r_n$ $x = x_n; y = y_n$

$$ax + my = \gcd(a, m) = 1.$$

Rewritten, this is

$$ax - 1 = (-y)m,$$

that is,

$$ax \equiv 1 \pmod{m},$$

so, a modular multiplicative inverse of a has been calculated. .