We will cover these parts of the book (8th edition):

4.1, 4.2
4.3.1-4.3.3
4.3.6-4.3.8
5.1

Now let us study some…

- Number Theory

Division

- Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.
- d is called divisor, a is called the dividend, q is called the quotient, and r is called the remainder. This notation is used to express the quotient and remainder:
- $q = a\ \boldsymbol{div}\ d, \qquad r = a\ \boldsymbol{mod}\ d$

UMASS BOSTON

The Division Algorithm

- **Example:**

- When we divide 17 by 5, we have

- $17 = 5 \cdot 3 + 2$.

- 17 is the dividend,
- 5 is the divisor,
- 3 is called the quotient, and
- 2 is called the remainder.

The Division Algorithm

- **Another example:**
- What happens when we divide -11 by 3 ?
- Note that the remainder cannot be negative.
- $-11 = 3 \cdot (-4) + 1$.

- -11 is the dividend,
- 3 is the divisor,
- -4 is called the quotient, and
- 1 is called the remainder.

Division

- If a and b are integers with a $\neq$ 0, we say that a **divides** b if there is an integer c so that b = ac.

- When a divides b we say that a is a **factor** of b and that b is a **multiple** of a.

- The notation **a | b** means that a divides b.

- We write **a X b** when a does not divide b.
- (see book for correct symbol).

Divisibility Theorems

- For integers a, b, and c it is true that

- if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
- **Example:** $3 \mid 6$ and $3 \mid 9$, so $3 \mid 15$.

- if $a \mid b$, then $a \mid bc$ for all integers c
- **Example:** $5 \mid 10$, so $5 \mid 20$, $5 \mid 30$, $5 \mid 40$, …

- if $a \mid b$ and $b \mid c$, then $a \mid c$
- **Example:** $4 \mid 8$ and $8 \mid 24$, so $4 \mid 24$.

- if $a \mid b$ and $a \mid c$, then $a \mid mb + nc$
- **Example:** $4 \mid 8$ and $4 \mid 12$, so $4 \mid 40$.

Modular Arithmetic

- Let a be an integer and m be a positive integer. We denote by **a mod m** the remainder when a is divided by m.

- **Examples:**

9 mod 4 = 1

9 mod 3 = 0

9 mod 10 = 9

-13 mod 4 = 3

Congruences

- Let a and b be integers and m be a positive integer. We say that **a is congruent to b modulo m** if m divides a – b.

- We use the notation **$a \equiv b \pmod{m}$** to indicate that a is congruent to b modulo m.

- In other words:
$a \equiv b \pmod{m}$ if and only if **a mod m = b mod m**.

UMASS BOSTON

Congruences

- **Examples:**
- Is it true that $46 \equiv 68 \pmod{11}$?
- Yes, because $11 \mid (46 - 68)$.
- Is it true that $46 \equiv 68 \pmod{22}$?
- Yes, because $22 \mid (46 - 68)$.
- For which integers z is it true that $z \equiv 12 \pmod{10}$?
- It is true for any $z \in \{\ldots, -28, -18, -8, 2, 12, 22, 32, \ldots\}$

- **Theorem:** Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Congruences

- **Theorem:** Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.
- **Proof:**
- We know that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies that there are integers s and t with $b = a + sm$ and $d = c + tm$.
- Therefore,
- $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
- $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.
- Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Congruences

- Let m be a positive integer and let a and b be integers. Then
  - $(a + b)\,\boldsymbol{mod}\,m = \big((a\,\boldsymbol{mod}\,m)$

Arithmetic Modulo m

- We can define arithmetic operations on $\boldsymbol{Z_m}$, the set of nonnegative integers less than m, that is, the set $\{0, 1, \ldots, m-1\}$:
- Addition: $a +_m b = (a + b)\ \boldsymbol{mod}\ m$
- Multiplication: $a \cdot_m b = (a \cdot b)\ \boldsymbol{mod}\ m$
- Example:
- $7 +_{11} 9 = (7 + 9)\ mod\ 11 = 16\ mod\ 11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9)\ mod\ 11 = 63\ mod\ 11 = 8$

UMASS BOSTON

Arithmetic Modulo m

- $+_m$ and $\cdot_m$ satisfy these properties: (if a,b,c belong to Z_m)
- **Closure**: $a +_m b$ and $a \cdot_m b$ belong to $\boldsymbol{Z_m}$
- **Associativity**: $(a +_m b) +_m c = a +_m (\mathrm{b} +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (\mathrm{b} \cdot_m c)$
- **Commutativity**: $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$
- **Identity elements**: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively. $a +_m 0 = 0 +_m a = a$ and $a \cdot_m 1 = 1 \cdot_m a = a$
- **Additive inverses**: If $a \neq 0$, then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- **Distributivity**: $a \cdot_m (\mathrm{b} +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

Representations of Integers

- Let b be a positive integer greater than 1.

Then if n is a positive integer, it can be expressed **uniquely** in the form:

- $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$,

- where k is a nonnegative integer,
- $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b,
- and $a_k \neq 0$.

- **Example for b=10:**
- $859 = 8 \cdot 10^2 + 5 \cdot 10^1 + 9 \cdot 10^0$

Representations of Integers

- **Example for b=2 (binary expansion):**
- $(10110)_2 = 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2^1 = (22)_{10}$
- **Example for b=16 (hexadecimal expansion):**
- (we use letters A to F to indicate numbers 10 to 15)
- $(3A0F)_{16} = 3 \cdot 16^3 + 10 \cdot 16^2 + 15 \cdot 16^0 = (14863)_{10}$
- **Example for b=8 (octal expansion)**
- $(7016)_8 = 7 \cdot 8^3 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$

Representations of Integers

- How can we construct the base b expansion of an integer n?
- First, divide n by b to obtain a quotient q_0 and remainder a_0, that is,
- $n = bq_0 + a_0$, where $0 \leq a_0 < b$.
- The remainder a_0 is the rightmost digit in the base b expansion of n.
- Next, divide q_0 by b to obtain:
- $q_0 = bq_1 + a_1$, where $0 \leq a_1 < b$.
- a_1 is the second digit from the right in the base b expansion of n. Continue this process until you obtain a quotient equal to zero.

UMASS BOSTON

Representations of Integers

- **Example:**

What is the base 8 expansion of $(12345)_{10}$?

- First, divide 12345 by 8:
- $12345 = 8 \cdot 1543 + 1$
- $1543 = 8 \cdot 192 + 7$
- $192 = 8 \cdot 24 + 0$
- $24 = 8 \cdot 3 + 0$
- $3 = 8 \cdot 0 + 3$
- The result is: $(12345)_{10} = (30071)_8$.

Representations of Integers

- **procedure** base_b_expansion(n, b: positive integers)
- q := n
- k := 0
- **while** q $\neq$ 0
- **begin**
-         a_k := q mod b
-         q := $\lfloor q/b \rfloor$
-         k := k + 1
- **end**
- **return** $(a_{k-1} \ldots a_1 a_0)$

{the base b expansion of n is $(a_{k-1} \ldots a_1 a_0)_b$ }

Conversion between Binary, Octal, and Hexadecimal expansion

- Conversion between binary and octal and between binary and hexadecimal expansions is extremely easy because each octal digit corresponds to a block of three binary digits and each hexadecimal digit corresponds to a block of four binary digits, with these correspondences shown below with these correspondences shown:

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Addition of Integers

- How do we (humans) add two integers?

- Example:

```
 1 1 1          carry
   7583
 + 4932
 ------
 1 2 5 1 5
```

Binary expansions:

```
      1   1            carry
      (1011)_2
  +   (1010)_2
  ------------
     (10101)_2
```

$(1011)_2 + (1010)_2 = (10101)_2$

Addition of Integers

- Let $a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2$, $b = (b_{n-1}b_{n-2}\ldots b_1b_0)_2$.
- How can we **algorithmically** add these two binary numbers?
- First, add their rightmost bits:
- $a_0 + b_0 = c_0 \cdot 2 + s_0$,
- where s_0 is the **rightmost bit** in the binary expansion of a + b, and c_0 is the **carry**.
- Then, add the next pair of bits and the carry:
- $a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1$,
- where s_1 is the **next bit** in the binary expansion of a + b, and c_1 is the carry.

Addition of Integers

- Continue this process until you obtain c_{n-1}.
- The leading bit of the sum is $s_n = c_{n-1}$.
- The result is:
- $a + b = (s_n s_{n-1} \ldots s_1 s_0)_2$

Addition of Integers

- **Example:**
- Add $a = (1110)_2$ and $b = (1011)_2$.
- $a_0 + b_0 = 0 + 1 = 0 \cdot 2 + 1$, so that $c_0 = 0$ and $s_0 = 1$.
- $a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 \cdot 2 + 0$, so $c_1 = 1$ and $s_1 = 0$.
- $a_2 + b_2 + c_1 = 1 + 0 + 1 = 1 \cdot 2 + 0$, so $c_2 = 1$ and $s_2 = 0$.
- $a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 \cdot 2 + 1$, so $c_3 = 1$ and $s_3 = 1$.
- $s_4 = c_3 = 1$.
- Therefore, $s = a + b = (11001)_2$.

Addition of Integers

- **procedure** add(a, b: positive integers)
- c := 0
- **for** j := 0 to n-1 {larger integer (a or b) has n digits}
- **begin**
-         d := $\lfloor (a_j + b_j + c)/2 \rfloor$
-         $s_j := a_j + b_j + c - 2d$
-         c := d
- **end**
- $s_n := c$
- **return** $(s_0 s_1 \ldots s_n)$

{the binary expansion of the sum is $(s_n s_{n-1} \ldots s_1 s_0)_2$}

Multiplication of Integers

- How do we (humans) multiply two integers?

- Example:

```
    7583
x     32
--------
   15166
+ 22749
--------
  242656
```

Binary expansions:

```
     110
x    101
--------
     110
    000
+  110
--------
   11110
```

Multiplication of Integers

- Let a = $(a_{n-1}a_{n-2}\ldots a_1a_0)_2$, b = $(b_{n-1}b_{n-2}\ldots b_1b_0)_2$.
- How can we **algorithmically** add these two binary numbers?
- The conventional algorithm works as follows. Using the distributive law, we see that:
- $ab = a(b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1})$
$= \quad a(b_0 2^0) + a(b_1 2^1) + \cdots + a(b_{n-1} 2^{n-1})$
- We first note that $ab_j = a$ if $b_j = 1$ and $ab_j = 0$ if $b_j = 0$. Each time we multiply a term by 2, we shift its binary expansion one place to the left and add a zero at the tail end of the expansion.

Multiplication of Integers

- Consequently, we can obtain $(ab_j)2^j$ by **shifting** the binary expansion of ab_j j places to the left, adding j zero bits at the tail end of this binary expansion. Finally, we obtain ab by adding the n integers ab_j2^j, $j = 0, 1, 2, \ldots, n-1$.

UMASS BOSTON

Multiplication of Integers

- **Example:**
- Product of a = $(110)_2$ and b = $(101)_2$.
- $ab_0 \cdot 2^0 = (110)_2 \cdot 1 \cdot 2^0 = (110)_2$
- $ab_1 \cdot 2^1 = (110)_2 \cdot 0 \cdot 2^1 = (0000)_2$
- $ab_2 \cdot 2^2 = (110)_2 \cdot 1 \cdot 2^2 = (11000)_2$

- Now add $(110)_2$, $(0000)_2$, and $(11000)_2$. Carrying out these additions shows that $ab = (11110)_2$

Multiplication of Integers

- **procedure** multiply(a, b: positive integers) {the binary expansions of a and b are $(a_{n-1}a_{n-2}\ldots a_1a_0)_2$ and $(b_{n-1}b_{n-2}\ldots b_1b_0)_2$ respectively}

- **for** j := 0 to n-1
- **if** $b_j = 1$ **then** $c_j := a$ shifted j places
- **else** $c_j := 0$ {$c_0, c_1, \ldots, c_{n-1}$ are the partial products}
- p := 0
- **for** j := 0 to n-1
- p := add(p, c_j)
- **return** p {p is the value of ab}

{the binary expansion of the sum is $(s_ns_{n-1}\ldots s_1s_0)_2$}

Fast modular exponentiation

- **Find b^n *mod* m.**
- First observe that we can avoid using large amount of memory if we compute $b^n \ \boldsymbol{mod}\ m$ by successively computing $b^k \ \boldsymbol{mod}\ m$ for $k = 1, 2, \ldots, n$ using the fact that $b^{k+1} \ \boldsymbol{mod}\ m = b\left(b^k \ \boldsymbol{mod}\ m\right) \boldsymbol{mod}\ m.$ However, this approach is impractical because it requires $n - 1$ multiplications of integers and n might be huge.

- **Faster way:**
- Suppose $n = (a_{k-1} \ldots a_1 a_0)_2$. First note that b^n $= b^{(a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0)} = b^{a_{k-1} \cdot 2^{k-1}} \cdot \ldots \cdot b^{a_1 \cdot 2} \cdot b^{a_0}$

Fast modular exponentiation

- This shows that to compute b^n, we need only compute the values of $b, b^2, (b^2)^2 = b^4, (b^4)^2 = b^8, \ldots, b^{2^k}$. Once we have these values, we multiply the terms b^{2^j} in this list, where $a_j = 1$.

- This gives us b^n. Then the algorithm finds $b\ \boldsymbol{mod}\ m$, $b^2\ \boldsymbol{mod}\ m$, $b^4\ \boldsymbol{mod}\ m$, …, $b^{2^{k-1}}\ \boldsymbol{mod}\ m$ and multiplies together those terms $b^{2^j}\ \boldsymbol{mod}\ m$ where $a_j = 1$, finding the remainder of the product when divided by m after each multiplication.

Fast modular exponentiation

- **procedure** modular_exponentiation(b: integer, $n = (a_{k-1}a_{k-2} \ldots a_1a_0)_2$, m: positive integer)

- $x := 1$
- $power := b \, \boldsymbol{mod} \, m$
- **for** i := 0 to k-1
- **begin**
- **if** $a_i = 1$ **then** $x := (x \cdot power) \, \boldsymbol{mod} \, m$
- $power := (power \cdot power) \, \boldsymbol{mod} \, m$
- **end**
- **return** x $\{x$ equals $b^n \, \boldsymbol{mod} \, m\}$

UMASS BOSTON

Fast modular exponentiation

- **Example**: find $3^{644}\ \boldsymbol{mod}\ 645$.
- $644 = (1010000100)_2$

$i = 0$: Because $a_0 = 0$, we have $x = 1$ and $power = 3^2 \textbf{ mod } 645 = 9 \textbf{ mod } 645 = 9$;

$i = 1$: Because $a_1 = 0$, we have $x = 1$ and $power = 9^2 \textbf{ mod } 645 = 81 \textbf{ mod } 645 = 81$;

$i = 2$: Because $a_2 = 1$, we have $x = 1 \cdot 81 \textbf{ mod } 645 = 81$ and $power = 81^2 \textbf{ mod } 645 = 6561 \textbf{ mod } 645 = 111$;

$i = 3$: Because $a_3 = 0$, we have $x = 81$ and $power = 111^2 \textbf{ mod } 645 = 12{,}321 \textbf{ mod } 645 = 66$;

$i = 4$: Because $a_4 = 0$, we have $x = 81$ and $power = 66^2 \textbf{ mod } 645 = 4356 \textbf{ mod } 645 = 486$;

$i = 5$: Because $a_5 = 0$, we have $x = 81$ and $power = 486^2 \textbf{ mod } 645 = 236{,}196 \textbf{ mod } 645 = 126$;

$i = 6$: Because $a_6 = 0$, we have $x = 81$ and $power = 126^2 \textbf{ mod } 645 = 15{,}876 \textbf{ mod } 645 = 396$;

$i = 7$: Because $a_7 = 1$, we find that $x = (81 \cdot 396) \textbf{ mod } 645 = 471$ and $power = 396^2 \textbf{ mod } 645 = 156{,}816 \textbf{ mod } 645 = 81$;

$i = 8$: Because $a_8 = 0$, we have $x = 471$ and $power = 81^2 \textbf{ mod } 645 = 6561 \textbf{ mod } 645 = 111$;

$i = 9$: Because $a_9 = 1$, we find that $x = (471 \cdot 111) \textbf{ mod } 645 = 36$.

Primes

- A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p.

- A positive integer that is greater than 1 and is not prime is called composite.

- The fundamental theorem of arithmetic:
- Every positive integer can be written **uniquely** as the **product of primes**, where the prime factors are written in order of increasing size.

Primes

- Examples:

$15 = 3 \cdot 5$

$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$

$17 = 17$

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

$512 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^9$

$515 = 5 \cdot 103$

$28 = 2 \cdot 2 \cdot 7 = 2^2 \cdot 7$

Primes

- If n is a composite integer, then n has a prime divisor less than or equal $\sqrt{n}$.

- This is easy to see: if n is a composite integer, it must have two divisors p_1 and p_2 such that $p_1 \cdot p_2 = n$ and $p_1 \geq 2$ and $p_2 \geq 2$.

- p_1 and p_2 cannot both be greater than $\sqrt{n}$, because then $p_1 \cdot p_2$ would be greater than n.

- If the smaller number of p_1 and p_2 is not a prime itself, then it can be broken up into prime factors that are smaller than itself but ≥ 2.

Greatest Common Divisors

- Let a and b be integers, not both zero.
- The largest integer d such that d | a and d | b is called the **greatest common divisor** of a and b.
- The greatest common divisor of a and b is denoted by gcd(a, b).
- **Example 1:** What is gcd(48, 72) ?
- The positive common divisors of 48 and 72 are 1, 2, 3, 4, 6, 8, 12, 16, and 24, so gcd(48, 72) = 24.
- **Example 2:** What is gcd(19, 72) ?
- The only positive common divisor of 19 and 72 is 1, so gcd(19, 72) = 1.

Greatest Common Divisors

- **Using prime factorizations:**
- $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$,
- where $p_1 < p_2 < \ldots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \leq i \leq n$
- $\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)}$
- **Example:**

$a = 60 = 2^2\ 3^1\ 5^1$

$b = 54 = 2^1\ 3^3\ 5^0$

$\gcd(a, b) = 2^1\ 3^1\ 5^0 = 6$

Relatively Prime Integers

- **Definition:**
- Two integers a and b are **relatively prime** if gcd(a, b) = 1.
- **Examples:**
- Are 15 and 28 relatively prime?
- Yes, gcd(15, 28) = 1.
- Are 55 and 28 relatively prime?
- Yes, gcd(55, 28) = 1.
- Are 35 and 28 relatively prime?
- No, gcd(35, 28) = 7.

Relatively Prime Integers

- **Definition:**
- The integers $a_1, a_2, \ldots, a_n$ are **pairwise relatively prime** if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

- **Examples:**
- Are 15, 17, and 27 pairwise relatively prime?
- No, because gcd(15, 27) = 3.

- Are 15, 17, and 28 pairwise relatively prime?
- Yes, because gcd(15, 17) = 1, gcd(15, 28) = 1 and gcd(17, 28) = 1.

UMASS BOSTON

Least Common Multiples

- **Definition:**
- The **least common multiple** of the positive integers a and b is the smallest positive integer that is divisible by both a and b.
- We denote the least common multiple of a and b by lcm(a, b).
- **Examples:**

lcm(3, 7) = 21

lcm(4, 6) = 12

lcm(5, 10) = 10

Least Common Multiples

- **Using prime factorizations:**
- $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$,
- where $p_1 < p_2 < \dots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \le i \le n$
- $\mathrm{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$
- **Example:**

$a = 60 = 2^2\ 3^1\ 5^1$

$b = 54 = 2^1\ 3^3\ 5^0$

$\mathrm{lcm}(a, b) = 2^2\ 3^3\ 5^1 = 4 □ 27 □ 5 = 540$

GCD and LCM

$a = 60 = 2^2 \; 3^1 \; 5^1$

$b = 54 = 2^1 \; 3^3 \; 5^0$

$\gcd(a, b) = 2^1 \; 3^1 \; 5^0 = 6$

$\text{lcm}(a, b) = 2^2 \; 3^3 \; 5^1 = 540$

Theorem: $ab = \gcd(a,b) \cdot \text{lcm}(a,b)$

The Euclidean Algorithm

- The **Euclidean Algorithm** finds the **greatest common divisor** of two integers a and b.
- For example, if we want to find gcd(287, 91), we **divide** 287 (the larger number) by 91 (the smaller one):
- $287 = 91 \cdot 3 + 14$

$\Rightarrow 287 - 91 \cdot 3 = 14$

$\Rightarrow 287 + 91 \cdot (-3) = 14$

- We know that for integers a, b and c,

if a | b, then a | bc for all integers c.

- Therefore, any divisor of 91 is also a divisor of $91 \cdot (-3)$.

The Euclidean Algorithm

287 + 91·(-3) = 14

- We also know that for integers a, b and c,
- **if a | b and a | c, then a | (b + c).**

- Therefore, any divisor of 287 and 91 must also be a divisor of 287 + 91·(-3), which is 14.

- Consequently, the greatest common divisor of **287 and 91** must be the same as the greatest common divisor of **14 and 91**:

- gcd(287, 91) = gcd(14, 91).

UMASS BOSTON

The Euclidean Algorithm

- In the next step, we divide 91 by 14:
- 91 = 14·6 + 7
- This means that gcd(14, 91) = gcd(14, 7).
- So we divide 14 by 7:
- 14 = 7·2 + 0
- We find that 7 | 14, and thus gcd(14, 7) = 7.
- **Therefore, gcd(287, 91) = 7**
- So we have this Lemma:
- **Let $a = bq + r$, where $a, b, q,$ and r are integers. Then $\mathbf{gcd}(a, b) = \mathbf{gcd}(b, r)$**

The Euclidean Algorithm

- In **pseudocode**, the algorithm can be implemented as follows:

- **procedure** gcd(a, b: positive integers)
- x := a
- y := b
- **while** y ≠ 0
- **begin**
-         r := x **mod** y
-         x := y
-         y := r
- **end**
- **return** x {x is gcd(a, b)}

GCDs as Linear Combinations

- **Bézout's Theorem**: If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.
- s and t are called Bézout's coefficients and the above equation is called Bézout's identity.

- We will see two methods to find the Bézout's identity of two integers.
    1. Working backward through the divisions of the Euclidean algorithm.
    2. Extended Euclidean algorithm

GCDs as Linear Combinations

- To run this extended Euclidean algorithm, we set $s_0 = 1$, $s_1 = 0, t_0 = 0$, and $t_1 = 1$ and let $s_j = s_{j-2} - q_{j-1}s_{j-1}$ and $t_j = t_{j-2} - q_{j-1}t_{j-1}$
- for $j = 2,3, \ldots, n$, where the q_j are the quotients in the divisions used when the Euclidean algorithm finds gcd(*a, b*).

GCDs as Linear Combinations

- Example for first method:

Express gcd(252, 198) = 18 as a linear combination of 252 and 198 by working backwards through the steps of the Euclidean algorithm.

Solution: To show that gcd(252, 198) = 18, the Euclidean algorithm uses these divisions:

$$252 = 198 \cdot 1 + 54$$
$$198 = 54 \cdot 3 + 36$$
$$54 = 36 \cdot 1 + 18$$
$$36 = 18 \cdot 2 + 0.$$

We summarize these steps in tabular form:

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	252	198	1	54
1	198	54	3	36
2	54	36	1	18
3	36	18	2	0

Using the next-to-last division (the third division), we can express gcd(252, 198) = 18 as a linear combination of 54 and 36. We find that

$$18 = 54 - 1 \cdot 36.$$

GCDs as Linear Combinations

The second division tells us that

$$36 = 198 - 3 \cdot 54.$$

Substituting this expression for 36 into the previous equation, we can express 18 as a linear combination of 54 and 198. We have

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$$

The first division tells us that

$$54 = 252 - 1 \cdot 198.$$

Substituting this expression for 54 into the previous equation, we can express 18 as a linear combination of 252 and 198. We conclude that

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198,$$

completing the solution. ◀

GCDs as Linear Combinations

- Example for second method:

Express gcd(252, 198) = 18 as a linear combination of 252 and 198 using the extended Euclidean algorithm.

Solution: Example 17 displays the steps the Euclidean algorithm uses to find gcd(252, 198) = 18. The quotients are $q_1 = 1$, $q_2 = 3$, $q_3 = 1$, and $q_4 = 2$. The desired Bézout coefficients are the values of s_4 and t_4 generated by the extended Euclidean algorithm, where $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, and $t_1 = 1$, and

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \qquad \text{and} \qquad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

for $j = 2, 3, 4$. We find that

$$s_2 = s_0 - s_1q_1 = 1 - 0 \cdot 1 = 1,\ t_2 = t_0 - t_1q_1 = 0 - 1 \cdot 1 = -1,$$
$$s_3 = s_1 - s_2q_2 = 0 - 1 \cdot 3 = -3,\ t_3 = t_1 - t_2q_2 = 1 - (-1)3 = 4,$$
$$s_4 = s_2 - s_3q_3 = 1 - (-3) \cdot 1 = 4,\ t_4 = t_2 - t_3q_3 = -1 - 4 \cdot 1 = -5.$$

Because $s_4 = 4$ and $t_4 = -5$, we see that $18 = \gcd(252, 198) = 4 \cdot 252 - 5 \cdot 198$.

GCDs as Linear Combinations

We summarize the steps of the extended Euclidean algorithm in a table:

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	−1
3	36	18	2	0	−3	4
4					4	−5

UMASS BOSTON

GCDs as Linear Combinations

Lemma: If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Proof:

$\gcd(a, b) = 1 \Rightarrow \exists s, t(sa + tb = 1) \Rightarrow sac + tbc = c$

We have $a|bc \Rightarrow a|tbc$ and we know that $a|sac$.

So we have $a|sac + tbc \Rightarrow a|c$

UMASS BOSTON

GCDs as Linear Combinations

Lemma: If p is a prime and $p|a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p|a_i$ for some i.

Proof:

By induction. (will be covered in the next sessions)

GCDs as Linear Combinations

Lemma: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Proof:

$ac \equiv bc \pmod{m} \Rightarrow m | ac - bc = c(a - b)$

Because $\gcd(c, m) = 1$, based on the previous lemma, we have $m | a - b \Rightarrow a \equiv b \pmod{m}$

Now it's Time for…

- **Induction and Recursion**

Induction

- The principle of mathematical induction is a useful tool for proving that a certain predicate is true for all natural numbers.
- It cannot be used to discover theorems, but only to prove them.
- To prove that propositional function $P(n)$ is true for all positive integers n, we complete two steps:

1. **Basis step**: Verify $P(1)$ (or $P(0)$) is true.
2. **Inductive step**: Show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

Induction

- **Example**: Show that $n < 2^n$ for all positive integers n.
- Let $P(n)$ be the proposition "$n < 2^n$“.
  1. Show that $P(1)$ is true.

     P(1) is true, because $1 < 2^1$
  2. Show that if $P(n)$ is true, then $P(n+1)$ is true

     Assume that $n < 2^n$ is true. We need to show that $P(n+1)$ is true, i.e. $n + 1 < 2^{n+1}$.

     We start from $\mathrm{P(n)}$: $n < 2^n \Rightarrow n + 1 < 2^n + 1 \leq 2^n + 2^n = 2^{n+1}$

     Therefor, if $n < 2^n$, then $n + 1 < 2^{n+1}$

So $n < 2^n$ is true for any positive integer.

Induction

- **Example**: $1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

1. Show that $P(1)$ is true.

   P(1) is true, because $1 = \frac{1*2}{2}$

2. Show that if $P(n)$ is true, then $P(n+1)$ is true

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \Rightarrow 1 + 2 + \cdots + n + (n+1)$$
$$= \frac{n(n+1)}{2} + (n+1) = (n+1)\left(\frac{n}{2} + 1\right)$$
$$= \frac{(n+1)(n+2)}{2} = \frac{(n+1)((n+1)+1)}{2}$$

So $P(n)$ is true for any positive integer.