Chapter 4: Properties of the Integers: Mathematical Induction

謝仁偉 助理教授
jenwei@mail.ntust.edu.tw
國立台灣科技大學 資訊工程系
2008 Fall

Outline

- ***The Well-Ordering Principle: Mathematical Induction***
- Recursive Definitions
- The Division Algorithm: Prime Numbers
- The Greatest Common Divisor: The Euclidean Algorithm
- The Fundamental Theorem of Arithmetic

The Well-Ordering Principle

- $\mathbf{Z}^+ = \{x \in \mathbf{Z} \mid x > 0\} = \{x \in \mathbf{Z} \mid x \geq 1\}$.
- $\mathbf{Q}^+ = \{x \in \mathbf{Q} \mid x > 0\}$ and $\mathbf{R}^+ = \{x \in \mathbf{R} \mid x > 0\}$
- ➡ We cannot represent $\mathbf{Q}^+$ or $\mathbf{R}^+$ using $\geq$ as we did for $\mathbf{Z}^+$. (If q is a positive rational number, then since $0 < q/2 < q$, we would have the smaller positive rational number $q/2$.)
- The Well-Ordering Principle: Every nonempty subset of $\mathbf{Z}^+$ contains a smallest element. (We often express this by saying that $\mathbf{Z}^+$ is well ordered.

The Principle of Mathematical Induction (1/3)

- **Theorem 4.1:** The Principle of Mathematical Induction. Let $S(n)$ denote an open mathematical statement (or set of such open statements) that involves one or more occurrences of the variable n, which repres tive integer.
  a) If $S(1)$ is true; and
  b) If whenever $S(k)$ is true (for some particular, but arbitrarily chosen, $k \in \mathbf{Z}^+$), then $S(k+1)$ is true;
  then $S(n)$ is true for all $n \in \mathbf{Z}^+$.

Basis step

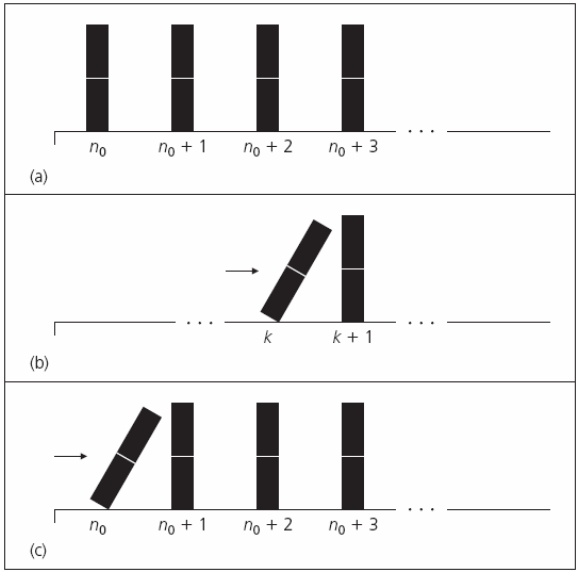
Inductive step

The Principle of Mathematical Induction (2/3)

- **Theorem 4.1 (cont.):**
  Proof. Let $F = \{t \in \mathbf{Z}^+ \mid S(t) \text{ is false}\}$.
  (want to prove that $F = \varnothing$)
  1) To obtain a contradiction, assume that $F \neq \varnothing$.
  By the Well-Ordering Principle, F has a least element m. Since $S(1)$ is true, $m \neq 1$, so $m > 1$.
  $m - 1 \in \mathbf{Z}^+$.
  2) With $m - 1 \notin F$, $S(m-1)$ is true.
  By condition (b), $S((m-1)+1) = S(m)$ is true.
  Contradicting $m \in F$. Consequently, $F = \varnothing$.

$$[S(n_0) \wedge [\forall k \geq n_0\, [S(k) \Rightarrow S(k+1)]]] \Rightarrow \forall n \geq n_0\, S(n).$$

The Principle of Mathematical Induction (3/3)



Examples (1/3)

- **Example 4.1:** Prove that for all $n \in \mathbf{Z}^+$,
$$\sum_{i=1}^{n} i = 1+2+3+\ldots+n = \frac{n(n+1)}{2}.$$
- **Example 4.3:** Among the 900 three-digit integers (from 100 to 999) those such as 131, 222, 303, 717, 848, and 969, where the integer is the same whether it is read from left to right or from right to left, are called palindromes. Without actually determining all of these three-digit palindromes, we would like to determine their sum.

Examples (2/3)

- **Example 4.3 (cont.):**

$$\begin{aligned}
\sum_{a=1}^{9}\left(\sum_{b=0}^{9} aba\right) &= \sum_{a=1}^{9}\sum_{b=0}^{9} aba = \sum_{a=1}^{9}\sum_{b=0}^{9}(101a+10b) \\
&= \sum_{a=1}^{9}\left[10(101a) + 10\sum_{b=0}^{9} b\right] = \sum_{a=1}^{9}\left[10(101a) + 10\sum_{b=1}^{9} b\right] \\
&= \sum_{a=1}^{9}\left[1010a + \frac{10(9\cdot 10)}{2}\right] = \sum_{a=1}^{9}(1010a + 450) \\
&= 1010\sum_{a=1}^{9} a + 9(450) \\
&= \frac{1010(9\cdot 10)}{2} + 4050 = 49{,}500.
\end{aligned}$$

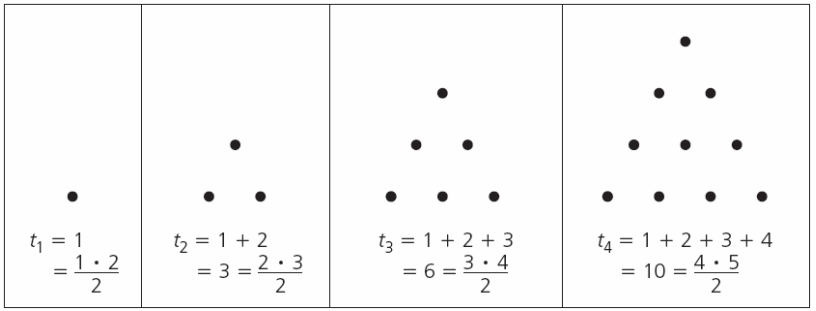
Example (3/3)

- **Example 4.4:** Prove that for each $n \in \mathbf{Z}^+$,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Triangular Numbers (1/2)

- **Example 4.5:** The figure below provides the first four entries of the sequence of triangular numbers. We see that $t_1 = 1$, $t_2 = 3$, $t_3 = 6$, $t_4 = 10$, and, in general, $t_i = 1 + 2 + \ldots + i = i(i+1)/2$, for each $i \in \mathbf{Z}^+$.



Triangular Numbers (2/2)

- **Example 4.5 (cont.):** For a fixed $n \in \mathbf{Z}^+$ we want a formula for the sum of the first n triangular numbers – that is, $t_1 + t_2 + \cdots + t_n = \sum_{i=1}^{n} t_i$.

  Considering n fixed (but arbitrary) we find that

$$\begin{aligned}\sum_{i=1}^{n} t_i &= \sum_{i=1}^{n} \frac{i(i+1)}{2} = \frac{1}{2}\sum_{i=1}^{n}(i^2+i) = \frac{1}{2}\sum_{i=1}^{n} i^2 + \frac{1}{2}\sum_{i=1}^{n} i \\ &= \frac{1}{2}\left[\frac{n(n+1)(2n+1)}{6}\right] + \frac{1}{2}\left[\frac{n(n+1)}{2}\right] = n(n+1)\left[\frac{2n+1}{12} + \frac{1}{4}\right] \\ &= \frac{n(n+1)(n+2)}{6}.\end{aligned}$$

The Need to Establish the Basis Step

- **Example 4.6:** If $n \in \mathbf{Z}^+$, establish the validity of the open statement

$$S(n): \quad \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n^2 + n + 2}{2}.$$

- What will happen if we go directly to the inductive step?
- Let us reconsider **Example 4.1**.

  $n(n+1) = n^2 + n + 2$ and $0 = 2$ (Something is wrong somewhere!)

➡ Remember to establish the basis step – no mater how easy it may be to verify it.

Efficient Procedures

```
procedure SumOfSquares1 (n: positive integer)
begin
   sum := 0
   for i := 1 to n do
      sum := sum + i^2
end
```

n additions and *n* multiplications

```
procedure SumOfSquares2 (n: positive integer)
begin
   sum := n * (n + 1) * (2 * n + 1)/6
end
```

2 additions + 3 multiplications + 1 division

Mathematical Induction Examples (1/3)

- **Example 4.7:** Consider the sums of consecutive odd positive integers.

1) 1	= 1	(= 1^2)
2) 1 + 3	= 4	(= 2^2)
3) 1 + 3 + 5	= 9	(= 3^2)
4) 1 + 3 + 5 + 7	= 16	(= 4^2)

Is the following result true?
For all $n \in \mathbf{Z}^+$,

$$S(n): \quad \sum_{i=1}^{n} (2i - 1) = n^2.$$

Mathematical Induction Examples (2/3)

- **Example 4.9:** The Harmonic numbers H_1, H_2, H_3 is defined as follows:

  $H_1 = 1$,
  $H_2 = 1 + 1/2$,
  $H_3 = 1 + 1/2 + 1/3$, …,

  and, in general, $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$, for each $n \in \mathbf{Z}^+$. Prove that for all $n \in \mathbf{Z}^+$,

$$\sum_{j=1}^{n} H_j = (n+1)H_n - n.$$

Hint: $H_k = H_{k+1} - 1/(k+1)$

Mathematical Induction Examples (3/3)

- **Example 4.13:** We learn from the equation 14 = 3 + 3 + 8 that we can express 14 using only 3's and 8's as summands. But what may prove to be surprising is that for all $n \geq 14$,
  $S(n)$: n can be written as a sum of 3's and/or 8's (with not regard to order).

Principle of Strong Mathematical Induction

- **Theorem 4.2:** The Principle of Mathematical Induction – Alternative Form. Let $S(n)$ denote an open mathematical statement (or set of such open statements) that involves one or more occurrences of the variable n, which represents a positive integer. Also let $n_0, n_1 \in \mathbf{Z}^+$ with $n_0 \leq n_1$.
  a) Basis Step: If $S(n_0)$, $S(n_0 + 1)$, $S(n_0 + 2)$, …, $S(n_1 - 1)$, and $S(n_1)$ are true; and
  b) Inductive Step: If whenever $S(n_0)$, $S(n_0 + 1)$, …, $S(k - 1)$, and $S(k)$ are true for some (particular but arbitrarily chosen) $k \in \mathbf{Z}^+$, where $k \geq n_1$, then the statement $S(k + 1)$ is also true;

  then $S(n)$ is true for all $n \geq n_0$.

Examples (1/2)

- **Example 4.14:** The following calculations indicate that it is possible to write (without regard to order) the integer 14, 15, 16 using only 3's and/or 8's as summands:
  $14 = 3 + 3 + 8$ $15 = 3 + 3 + 3 + 3 + 3$ $16 = 8 + 8$
  On the basis of these three results, we make the conjecture: For every $n \in \mathbf{Z}^+$ where $n \geq 14$, $S(n)$: n can be written as a sum of 3's and/or 8's.

Examples (2/2)

- **Example 4.15:** Let us consider the integer sequence $a_0, a_1, a_2, a_3, \ldots$, where $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, and $a_n = a_{n-1} + a_{n-2} + a_{n-3}$, for all $n \in \mathbf{Z}^+$ where $n \geq 3$. (Then, for instance, we find that $a_3 = a_2 + a_1 + a_0 = 3 + 2 + 1 = 6$; $a_4 = a_3 + a_2 + a_1 = 6 + 3 + 2 = 11$; and $a_5 = a_4 + a_3 + a_2 = 11 + 6 + 3 = 20$.)
  We claim that the entries in this sequence are such that $a_n \leq 3^n$ for all $n \in \mathbf{N}$ – that is, $\forall n \in \mathbf{N}$ $S'(n)$, where $S'(n)$ is the open statement: $a_n \leq 3^n$.
- **EXERCISES 4.1:** 18, 24

Outline

- The Well-Ordering Principle: Mathematical Induction
- ***Recursive Definitions***
- The Division Algorithm: Prime Numbers
- The Greatest Common Divisor: The Euclidean Algorithm
- The Fundamental Theorem of Arithmetic

Explicit Formula (1/3)

- Consider the integer sequence $b_0, b_1, b_2, b_3, \ldots$, where $b_n = 2n$ for all $n \in \mathbf{N}$.
- If we need to determine b_6, we simply calculate $b_6 = 2 \cdot 6 = 12$ – without the need to calculate the value of b_n for any other $n \in \mathbf{N}$.
- We can perform such calculations because we have an explicit formula – namely, $b_n = 2n$ – that tells us how b_n is determined from n (alone).

Explicit Formula (2/3)

- Consider the integer sequence $a_0, a_1, a_2, a_3, \ldots$, where
  $a_0 = 1, a_1 = 2, a_2 = 3,$ and
  $a_n = a_{n-1} + a_{n-2} + a_{n-3},$ for all $n \in \mathbf{Z}^+$ where $n \geq 3$.
- If we want the value of a_6, we need to know the values of a_5, a_4, and a_3. (Because we do not have an explicit formula that defines each a_n in terms of n for all $n \in \mathbf{N}$.)

Explicit Formula (3/3)

$$
\begin{aligned}
a_6 &= a_5 + a_4 + a_3 \\
&= (a_4 + a_3 + a_2) + (a_3 + a_2 + a_1) + (a_2 + a_1 + a_0) \\
&= [(a_3 + a_2 + a_1) + (a_2 + a_1 + a_0) + a_2] \\
&\quad + [(a_2 + a_1 + a_0) + a_2 + a_1] + (a_2 + a_1 + a_0) \\
&= [[(a_2 + a_1 + a_0) + a_2 + a_1] + (a_2 + a_1 + a_0) + a_2] \\
&\quad + [(a_2 + a_1 + a_0) + a_2 + a_1] + (a_2 + a_1 + a_0) \\
&= [[(3 + 2 + 1) + 3 + 2] + (3 + 2 + 1) + 3] \\
&\quad + [(3 + 2 + 1) + 3 + 2] + (3 + 2 + 1) \\
&= 37.
\end{aligned}
$$

Recursive Definition

- For the sequence $a_0, a_1, a_2, a_3, \ldots$, we may be able to define what we need in terms of similar prior results.
- When we do so we say that the concept is defined recursively, using the method, or process, of recursion.

Examples of Recursive Definition

- Harmonic numbers $H_1, H_2, H_3, \ldots$
  1) $H_1 = 1$; and
  2) For $n \geq 1$, $H_{n+1} = H_n + \left(\frac{1}{n+1}\right)$.
- $n!$
  1) $0! = 1$; and
  2) For $n \geq 0$, $(n+1)! = (n+1)(n!)$.
- Explicit formula $b_n = 2n$, $n \in \mathbf{N}$.
  1) $b_0 = 0$; and
  2) For $n \geq 0$, $b_{n+1} = b_n + 2$.

The Fibonacci Numbers (1/2)

- **Example 4.19:** The Fibonacci numbers may be defined recursively by
  1) $F_0 = 0$, $F_1 = 1$; and
  2) $F_n = F_{n-1} + F_{n-2}$, for $n \in \mathbf{Z}^+$ with $n \geq 2$.

  Hence, from the recursive part of this definition, it follows that

$$F_2 = F_1 + F_0 = 1 + 0 = 1 \qquad F_4 = F_3 + F_2 = 2 + 1 = 3$$
$$F_3 = F_2 + F_1 = 1 + 1 = 2 \qquad F_5 = F_4 + F_3 = 3 + 2 = 5.$$

The Fibonacci Numbers (2/2)

- Let us consider the following five results that deal with sums of squares of the Fibonacci numbers.

1) $F_0^2 + F_1^2 = 0^2 + 1^2 = 1 = 1 \times 1$
2) $F_0^2 + F_1^2 + F_2^2 = 0^2 + 1^2 + 1^2 = 2 = 1 \times 2$
3) $F_0^2 + F_1^2 + F_2^2 + F_3^2 = 0^2 + 1^2 + 1^2 + 2^2 = 6 = 2 \times 3$
4) $F_0^2 + F_1^2 + F_2^2 + F_3^2 + F_4^2 = 0^2 + 1^2 + 1^2 + 2^2 + 3^2 = 15 = 3 \times 5$
5) $F_0^2 + F_1^2 + F_2^2 + F_3^2 + F_4^2 + F_5^2 = 0^2 + 1^2 + 1^2 + 2^2 + 3^2 + 5^2 = 40 = 5 \times 8$

From what is suggested in these calculations, we conjecture that

$$\forall n \in \mathbf{Z}^+ \sum_{i=0}^{n} F_i^2 = F_n \times F_{n+1}.$$

The Lucas Numbers

- **Example 4.20:** The Lucas numbers is defined by
  1) $L_0 = 2$, $L_1 = 1$; and
  2) $L_n = L_{n-1} + L_{n-2}$, for $n \in \mathbf{Z}^+$ with $n \geq 2$.

n	0	1	2	3	4	5	6	7
L_n	2	1	3	4	7	11	18	29

One of the interrelations between the Fibonacci and Lucas numbers is illustrated in the fact that

$$\forall n \in \mathbf{Z}^+ \; L_n = F_{n-1} + F_{n+1}.$$

The Eulerian Numbers (1/3)

- **Example 4.21:** For $m, k \in \mathbf{N}$, the Eulerian numbers $a_{m,k}$ are defined recursively by

$$a_{m,k} = (m-k)a_{m-1,k-1} + (k+1)a_{m-1,k}, \quad 0 \le k \le m-1,$$
$$a_{0,0} = 1, \quad a_{m,k} = 0, \quad k \ge m, \quad a_{m,k} = 0, \quad k < 0.$$

The values for $a_{m,k}$, where $1 \le m \le 5$ and $0 \le k \le m-1$, are given as follows:

						Row Sum
$(m=1)$			1			$1 = 1!$
$(m=2)$		1		1		$2 = 2!$
$(m=3)$	1		4		1	$6 = 3!$
$(m=4)$	1	11		11	1	$24 = 4!$
$(m=5)$	1	26	66	26	1	$120 = 5!$

The Eulerian Numbers (2/3)

- **Example 4.21 (cont.):** These results suggest that for a fixed $m \in \mathbf{Z}^+$, $\sum_{k=0}^{m-1} a_{m,k} = m!$, the number of permutations of m objects taken m at a time.

  Assuming the result true for some fixed m (≥ 1), we find that

$$\begin{aligned}\sum_{k=0}^{m} a_{m+1,k} &= \sum_{k=0}^{m} [(m+1-k)a_{m,k-1} + (k+1)a_{m,k}] \\ &= [(m+1)a_{m,-1} + a_{m,0}] + [ma_{m,0} + 2a_{m,1}] + [(m-1)a_{m,1} + 3a_{m,2}] + \cdots \\ &\quad + [3a_{m,m-3} + (m-1)a_{m,m-2}] + [2a_{m,m-2} + ma_{m,m-1}] \\ &\quad + [a_{m,m-1} + (m+1)a_{m,m}].\end{aligned}$$

The Eulerian Numbers (3/3)

- **Example 4.21 (cont.):** Since $a_{m,-1} = 0 = a_{m,m}$ we can write

$$\begin{aligned}\sum_{k=0}^{m} a_{m+1,k} &= [a_{m,0} + ma_{m,0}] + [2a_{m,1} + (m-1)a_{m,1}] + \cdots \\ &\quad + [(m-1)a_{m,m-2} + 2a_{m,m-2}] + [ma_{m,m-1} + a_{m,m-1}] \\ &= (m+1)\sum_{k=0}^{m-1} a_{m,k} = (m+1)m! = (m+1)!\end{aligned}$$

Consequently, the result is true for all $m \ge 1$ – by the Principle of Mathematical Induction.

Recursively Defined Set

- A recursively defined set X:
  - Start with an initial collection of elements that are in X – this provides the base of the recursion.
  - A rule or list of rules tell us how to find new elements in X from other elements already known to be in X.
- **Example 4.22:** Define the set X recursively by
  1) $1 \in X$; and
  2) For each $a \in X$, $a + 2 \in X$.
  Then we claim that X consists (precisely) of all positive odd integers.
- **EXERCISES 4.2:** 12, 16

Outline

- The Well-Ordering Principle: Mathematical Induction
- Recursive Definitions
- ***The Division Algorithm: Prime Numbers***
- The Greatest Common Divisor: The Euclidean Algorithm
- The Fundamental Theorem of Arithmetic

Properties of Division Operation (1/3)

- **Definition 4.1:** If $a, b \in \mathbf{Z}$ and $b \neq 0$, we say that b divides a, and we write $b|a$, if there is an integer n such that $a = bn$. When this occurs we say that b is a divisor of a, or a is a multiple of b.
- **Theorem 4.3:** For all $a, b, c \in \mathbf{Z}$

  a) $1 \mid a$ and $a \mid 0$.

  b) $[(a \mid b) \wedge (b \mid a)] \Rightarrow a = \pm b$.

  c) $[(a \mid b) \wedge (b \mid c)] \Rightarrow a \mid c$.

  d) $a \mid b \Rightarrow a \mid bx$ for all $x \in \mathbf{Z}$.

Properties of Division Operation (2/3)

- **Theorem 4.3 (cont.):**

  e) If $x = y + z$, and a divides two of the three integers x, y, and z, then a divides the remaining integer.

  f) $[(a \mid b) \wedge (a \mid c)] \Rightarrow a \mid (bx + cy)$, for all $x, y \in \mathbf{Z}$. (The expression $bx + cy$ is called a linear combination of b, c.)

Properties of Division Operation (3/3)

- **Theorem 4.3 (cont.):**

  g) For $1 \leq i \leq n$, let $c_i \in \mathbf{Z}$. If a divides each c_i, then $a \mid (c_1 x_1 + c_2 x_2 + \cdots + c_n x_n)$, where $x_i \in \mathbf{Z}$ for all $1 \leq i \leq n$.

Proof: f) If $a \mid b$ and $a \mid c \Rightarrow b = am$ and $c = an$, for some $m, n \in \mathbf{Z}$.

$\therefore bx + cy = (am)x + (an)y = a(mx + ny)$

$\therefore a \mid (bx + cy)$

Example

- **Example 4.24:** Let $a, b \in \mathbf{Z}$ so that $2a + 3b$ is a multiple of 17. (For example, we could have $a = 7$ and $b = 1$ – and $a = 4$, $b = 3$ also works.) Prove that 17 divides $9a + 5b$.

  Proof:

  $17 \mid (2a + 3b) \Rightarrow 17 \mid (-4)(2a + 3b)$, by part (d)

  $17 \mid (17a + 17b)$, by part (f)

  $17 \mid [(17a + 17b) + (-4)(2a + 3b)]$, by part (e)

  Consequently, we have $17 \mid (9a + 5b)$.

Prime and Composite (1/3)

- Number theory is now an essential applicable tool in dealing with computer and Internet security.
- Primes are the positive integers that have only two positive divisors, namely, 1 and n itself. All other positive integers are called composite.
- **Lemma 4.1:** If $n \in \mathbf{Z}^+$ and n is composite, then there is a prime p such that $p|n$.

  Proof: If no such a prime, let S be the set of all composite integers that have no prime divisors.

Prime and Composite (2/3)

- **Lemma 4.1 (cont.):**

  By Well-Ordering Principle, S has a least element m.

  If m is composite, then $m = m_1 m_2$, where $m_1, m_2 \in \mathbf{Z}^+$ with $1 < m_1 < m$ and $1 < m_2 < m$.

  Since $m_1 \notin S$, m_1 is prime or divisible by a prime, so exists a prime p such that $p|m_1$.

  Since $p|m_1$ and $m = m_1 m_2$, so $p|m$ and $S = \varnothing$ (contradiction, **Theorem 4.3** (d)).

Prime and Composite (3/3)

- **Theorem 4.4:** (Euclid) There are infinitely many primes.

  Proof: If not, let $p_1, p_2, \ldots, p_k$ be the finite list of all primes, and let $B = p_1 p_2 \ldots p_k + 1$.

  Since $B > p_i$, for all $1 \le i \le k$, B cannot be a prime.

  Hence B is composite, $p_j|B$, $1 \le j \le k$ (**Lemma 4.1**)

  Since $p_j|B$ and $p_j|p_1 p_2 \ldots p_k$, so $p_j|1$. (Contradiction, **Theorem 4.3** (e))

The Division Algorithm (1/3)

- **Theorem 4.5:** The Division Algorithm. If $a, b \in \mathbf{Z}$, with $b > 0$, then there exist unique $q, r \in \mathbf{Z}$ with $a = qb + r$, $0 \le r < b$.

  Proof: If $b \mid a$ the result follows with $r = 0$, so consider the case where $b \nmid a$ (b does not divide a).

  q, r exist

  Let $S = \{a - tb \mid t \in \mathbf{Z}, a - tb > 0\}$.

  $r > 0$

  (i) If $a > 0$ and $t = 0$, then $a \in S$ and $S \neq \varnothing$.

  (ii) If $a \le 0$ and let $t = a - 1$, then $a - tb = a - (a - 1)b = a(1 - b) + b$. $\because (1 - b) \le 0$ $\therefore a - tb > 0$ and $S \neq \varnothing$.

The Division Algorithm (2/3)

- **Theorem 4.5 (cont.):**

  $\because S \neq \varnothing$ $\therefore S$ has a least element r, where $0 < r = a - qb$, for some $q \in \mathbf{Z}$ (Well-Ordering Principle)

  (i) If $r = b$, then $a = (q + 1)b$, contradicting $b \nmid a$.

  (ii) If $r > b$, then $r = b + c$, for some $c \in \mathbf{Z}^+$, and $a - qb = r = b + c \Rightarrow c = a - (q + 1)b \in S$, contradicting r being the least element of S.

  Hence, $r < b$.

The Division Algorithm (3/3)

- **Theorem 4.5 (cont.):**

  q, r unique

  If there are other q's and r's, let $q_1, q_2, r_1, r_2 \in \mathbf{Z}$ with $a = q_1 b + r_1$, for $0 \le r_1 < b$, and $a = q_2 b + r_2$, for $0 \le r_2 < b$.

  Then $q_1 b + r_1 = q_2 b + r_2 \Rightarrow b|q_1 - q_2| = |r_1 - r_2| < b$, contradicting if $q_1 \neq q_2$. Hence, $q_1 = q_2$, $r_1 = r_2$.

When $a, b \in \mathbf{Z}$, with $b > 0$, then there exists a unique quotient q and a unique remainder r where $a = qb + r$, with $0 \le r < b$. The integer b is called the divisor while a is termed the dividend.

Example (1/2)

- **Example 4.25:**

  a) If the dividend $a = 170$ and the divisor $b = 11$, then the quotient $q = 15$, and the remainder $r = 5$. $(170 = 15 \times 11 + 5)$

  b) If the dividend $a = 98$ and the divisor $b = 7$, then the quotient $q = 14$, and the remainder $r = 0$. $(98 = 14 \times 7)$

  c) If the dividend $a = -45$ and the divisor $b = 8$, what are the quotient and the remainder?

  $-45 = (-6) \times 8 + 3$ vs. $-45 = (-5) \times 8 - 5$

Example (2/2)

- **Example 4.25 (cont.):**
  d) Let $a, b \in \mathbf{Z}$,

  1) If $a = qb$ for some $q \in \mathbf{Z}^+$, then $-a = (-q)b$. So, when $-a$ (< 0) is divided by b (> 0) the quotient is $-q$ (< 0) and the remainder is 0.

  2) If $a = qb + r$ for some $q \in \mathbf{N}$ and $0 < r < b$, then $-a = (-q)b - r = (-q - 1)b + (b - r)$. So, the quotient is $-q - 1$, and the remainder is $b - r$, where $0 < b - r < b$.

Pseudo Code (1/2)

```
procedure IntegerDivision (a, b: integers)
begin
  if a = 0 then
    begin
      quotient := 0
      remainder := 0
    end
  else
    begin
      r := abs(a) {the absolute value of a}
      q := 0
      while r ≥ b do
        begin
          r := r - b
          q := q + 1
        end
```


Pseudo Code (2/2)

```
      if a > 0 then
        begin
          quotient := q
          remainder := r
        end
      else if r = 0 then
        begin
          quotient := -q
          remainder := 0
        end
      else
        begin
          quotient := -q - 1
          remainder := b - r
        end
    end
end
```


Octal System

- **Example 4.27:** Write 6137 in the octal system (base 8). Here we seek nonnegative integers r_0, $r_1, r_2, \ldots, r_k$, with $0 < r_k < 8$, such that $6137 = (r_k \ldots r_2 r_1 r_0)_8$.
  $6137 = (13771)_8$

Hexadecimal (Base-16) Number System

Base 10	Base 2	Base 16	Base 10	Base 2	Base 16
0	0 0 0 0	0	8	1 0 0 0	8
1	0 0 0 1	1	9	1 0 0 1	9
2	0 0 1 0	2	10	1 0 1 0	A
3	0 0 1 1	3	11	1 0 1 1	B
4	0 1 0 0	4	12	1 1 0 0	C
5	0 1 0 1	5	13	1 1 0 1	D
6	0 1 1 0	6	14	1 1 1 0	E
7	0 1 1 1	7	15	1 1 1 1	F

- Represent the (base-10) integer 13,874,945 in the hexadecimal system.
  $(D3B701)_{16}$

Convert between Base 2 and Base 16

- $(01001101)_2 = (4D)_{16}$

$$\underbrace{0100}_{4} \quad \underbrace{1101}_{D}$$

- $(A13F)_{16} = (1010000100111111)_2$

$$\underbrace{A}_{1010} \quad \underbrace{1}_{0001} \quad \underbrace{3}_{0011} \quad \underbrace{F}_{1111}$$

Two's Complement Method (1/2)

To obtain the four-bit patterns for $-8 \le n \le -1$, do the following:

1. Replace each 0(1) in the binary representation of $|n|$ by 1(0). (one's complement of $|n|$)
2. Add 1 (=0001 in this case) to the result in step (1). (two's complement of $|n|$)

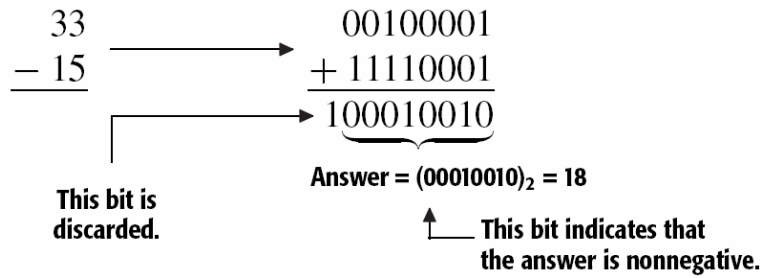
Two's Complement Method (2/2)

Two's Complement Notation	
Value Represented	Four-Bit Pattern
7	0 1 1 1
6	0 1 1 0
5	0 1 0 1
4	0 1 0 0
3	0 0 1 1
2	0 0 1 0
1	0 0 0 1
0	0 0 0 0
−1	1 1 1 1
−2	1 1 1 0
−3	1 1 0 1
−4	1 1 0 0
−5	1 0 1 1
−6	1 0 1 0
−7	1 0 0 1
−8	1 0 0 0

Subtraction in Base 2 (1/3)

- **Example 4.30:** How do we perform the subtraction 33 – 15 in base 2, using the two's complement method with patterns of eight bits (= one byte)?

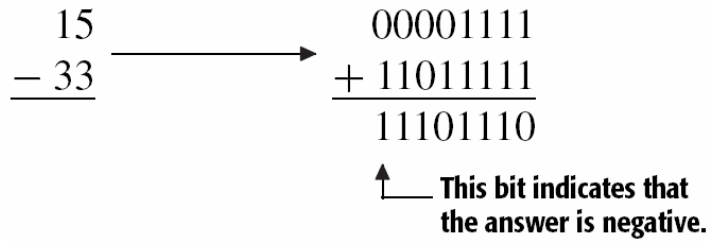
  33 – 15 = 33 + (–15)



Subtraction in Base 2 (2/3)

- **Example 4.30 (cont.):**

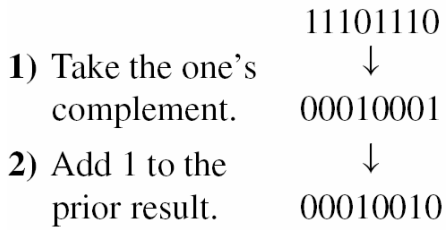
  To find 15 – 33 we use 15 = $(00001111)_2$ and 33 = $(00100001)_2$.



Subtraction in Base 2 (3/3)

- **Example 4.30 (cont.):**

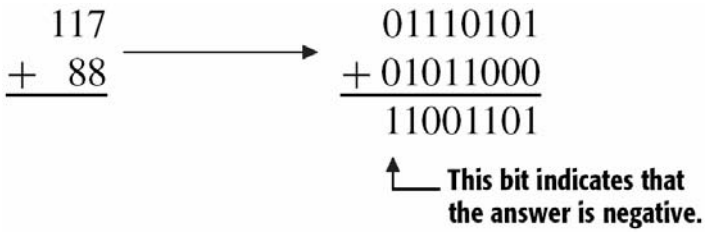
  In order to get the positive form of the answer, we proceed as follows:



  Since $(00010010)_2$ = 18, the answer is –18.

Overflow Error

- When we exceed the size of the integers that can be represented, an overflow error results.



Here an overflow error is indicated: The sum of the eight-bit patterns for two positive (negative) integers has resulted in the eight-bit pattern for a negative (positive) integer.

One Result on Composite Integers (1/2)

- **Example 4.31:** If $n \in \mathbf{Z}^+$ and n is composite, then there exists a prime p such that $p|n$ and $p \leq \sqrt{n}$.

  Proof:

  Since n is a composite, we can write $n = n_1 n_2$, where $1 < n_1 < n$ and $1 < n_2 < n$.

  We claim that one of n_1 , n_2 must be less than or equal to $\sqrt{n}$.

  If not, then $n_1 > \sqrt{n}$ and $n_2 > \sqrt{n}$ give us a contradiction $n = n_1 n_2 > (\sqrt{n})(\sqrt{n}) = n$.

One Result on Composite Integers (2/2)

- **Example 4.31 (cont.):**

  Without loss of generality, we assume $n_1 \leq \sqrt{n}$.

  (i) If n_1 is prime, the statement is true.

  (ii) If n_1 is not prime, then by Lemma 4.1 there exists a prime $p < n_1$ where $p|n_1$.

  So $p|n$ and $p \leq \sqrt{n}$.

- **EXERCISES 4.3:** 10, 12, 18

Outline

- The Well-Ordering Principle: Mathematical Induction
- Recursive Definitions
- The Division Algorithm: Prime Numbers
- ***The Greatest Common Divisor: The Euclidean Algorithm***
- The Fundamental Theorem of Arithmetic

Common Divisor

- **Definition 4.2:** For $a, b \in \mathbf{Z}$, a positive integer c is said to be a common divisor of a and b if $c|a$ and $c|b$.
- **Example 4.32:** The common divisors of 42 and 70 are 1, 2, 7, and 14, and 14 is the greatest of the common divisors.

Greatest Common Divisor

- **Definition 4.3:** Let $a, b \in \mathbf{Z}$, where either $a \neq 0$ or $b \neq 0$. Then $c \in \mathbf{Z}^+$ is called a greatest common divisor of a, b if
  a) $c|a$ and $c|b$
  b) for any common divisor d of a and b, we have $d|c$.
- **Questions:**
  - Does a greatest common divisor of a and b always exist?
  - What would we deal with greatest common divisors for large integers a and b?

Uniqueness of GCD (1/2)

- **Theorem 4.6:** For all $a, b \in \mathbf{Z}^+$, there exists a unique $c \in \mathbf{Z}^+$ that is the greatest common divisor of a, b.

  Proof: Given $a, b \in \mathbf{Z}^+$, let $S = \{as + bt \mid s, t \in \mathbf{Z}, as + bt > 0\}$. Since $S \neq \varnothing$, by the Well-Ordering Principle S has a least element c.

  (i) *Existence*: We claim that c is a greatest common divisor of a, b.
  - Since $c \in S$, $c = ax + by$, for some $x, y \in \mathbf{Z}$.

  ➡ Consequently, if $d \in \mathbf{Z}$ and $d|a$ and $d|b$, then by **Theorem 4.3** (f) $d|(ax + by)$, so $d|c$.

Uniqueness of GCD (2/2)

- **Theorem 4.6 (cont.):**
  - If $c \nmid a$, $a = qc + r$, with $q, r \in \mathbf{Z}^+$ and $0 < r < c$.
    Then $r = a - qc = a - q(ax + by) = (1 - qx)a + (-qy)b$
    $r \in S$, contradicting the choice of c as the least element of S.

  ➡ Consequently, $c|a$, and by similar argument, $c|b$.

  ➡ Hence all $a, b \in \mathbf{Z}^+$ have a greatest common divisor.

  (ii) *Uniqueness*: If c_1, c_2 both satisfy **Definition 4.3**, then $c_2|c_1$ and $c_2|c_1$.

➡ We conclude from **Theorem 4.3** (b) that $c_1 = c_2$ because $c_1, c_2 \in \mathbf{Z}^+$.

Properties of Greatest Common Divisor

- The greatest common divisor of a, b is denoted by $\gcd(a, b)$.
  - $\gcd(a, b) = \gcd(b, a)$
  - For each $a \in \mathbf{Z}$, if $a \neq 0$, then $\gcd(a, 0) = |a|$
  - When $a, b \in \mathbf{Z}$, $\gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b) = \gcd(a, b)$
  - $\gcd(0, 0)$ is not defined and is of no interest to us.
  - $\gcd(a, b)$ is the smallest positive integer we can write as a linear combination of a and b.
  - Integers a and b are called relatively prime when $\gcd(a, b) = 1$ – that is, when there exist $x, y \in \mathbf{Z}$ with $ax + by = 1$.

Example

- **Example 4.33:** Since $\gcd(42, 70) = 14$, we can find $x, y \in \mathbf{Z}$ with $42x + 70y = 14$, or $3x + 5y = 1$. Is the solution for x, y *unique*?

  By inspection $x = 2$, $y = -1$ is a solution.

  But for $k \in \mathbf{Z}$, $1 = 3(2 - 5k) + 5(-1 + 3k)$, so $14 = 42(2 - 5k) + 70(-1 + 3k)$, and the solutions for x, y are not unique.
- In general, if $\gcd(a, b) = d$, then $\gcd((a/d), (b/d)) = 1$. If $(a/d)x_0 + (b/d)y_0 = 1$, then $1 = (a/d)(x_0 - (b/d)k) + (b/d)(y_0 + (a/d)k)$, for each $k \in \mathbf{Z}$. So $d = a(x_0 - (b/d)k) + b(y_0 + (a/d)k)$, yielding infinitely many solutions to $ax + by = d$.

Euclidean Algorithm (1/3)

- **Theorem 4.7:** Euclidean Algorithm. Let $a, b \in \mathbf{Z}^+$. Set $r_0 = a$ and $r_1 = b$ and apply the division algorithm n times as follows:

$$
\begin{aligned}
r_0 &= q_1 r_1 + r_2, && 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, && 0 < r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4, && 0 < r_4 < r_3 \\
&\cdots \\
r_i &= q_{i+1} r_{i+1} + r_{i+2}, && 0 < r_{i+2} < r_{i+1} \\
&\cdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n, && 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n.
\end{aligned}
$$

Euclidean Algorithm (2/3)

- **Theorem 4.7 (cont.):**

  Then r_n, the last nonzero remainder, equals $\gcd(a, b)$.

  Proof: To verify that $r_n = \gcd(a, b)$, we establish the two definitions of **Definition 4.3**.

  (i) Verify $c|r_n$ for any common divisor c of a and b

  If $c|r_0$ and $c|r_1$, then as $r_0 = q_1 r_1 + r_2$, it follows $c|r_2$.

  Next $[(c|r_1) \wedge (c|r_2)] \Rightarrow c|r_3$

  Continuing down $\Rightarrow c|r_n$

Euclidean Algorithm (3/3)

- **Theorem 4.7 (cont.):**

  (ii) Verify $r_n|a$ and $r_n|b$

  Since $r_n|r_{n-1}$ and $r_{n-2} = q_{n-1}r_{n-1} + r_n$, we have $r_n|r_{n-2}$.

  Continuing up through the equations, we get to where $r_n|r_4$ and $r_n|r_3$, so $r_n|r_2$.

  Then $[(r_n|r_3) \wedge (r_n|r_2)] \Rightarrow r_n|r_1$ (that is, $r_n|b$).

  Finally, $[(r_n|r_2) \wedge (r_n|r_1)] \Rightarrow r_n|r_0$ (that is, $r_n|a$).

➡ Hence, $r_n = \gcd(a, b)$.

Example (1/2)

- **Example 4.34:** Find the greatest common divisor of 250 and 111, and express the result as a linear combination of these integers.

$$\begin{aligned} 250 &= 2(111) + 28, & 0 < 28 < 111 \\ 111 &= 3(28) + 27, & 0 < 27 < 28 \\ 28 &= 1(27) + 1, & 0 < 1 < 27 \\ 27 &= 27(1) + 0. \end{aligned}$$

gcd(250, 111) = 1

250 and 111 are relatively prime.

$1 = 250[4 - 111k] + 111[-9 + 250k]$, for any $k \in \mathbf{Z}$.

Example (2/2)

- **Example 4.35:** For any $n \in \mathbf{Z}^+$, prove that the integers $8n + 3$ and $5n + 2$ are relatively prime.

When $n = 1$ we find that $\gcd(8n + 3, 5n + 2) = \gcd(11, 7) = 1$.

For $n \geq 2$ we have $8n + 3 > 5n + 2$, we may write

$$\begin{aligned} 8n + 3 &= 1(5n + 2) + (3n + 1), & 0 < 3n + 1 < 5n + 2 \\ 5n + 2 &= 1(3n + 1) + (2n + 1), & 0 < 2n + 1 < 3n + 1 \\ 3n + 1 &= 1(2n + 1) + n, & 0 < n < 2n + 1 \\ 2n + 1 &= 2(n) + 1, & 0 < 1 < n \\ n &= n(1) + 0. \end{aligned}$$

Consequently, the last nonzero remainder is 1, so $\gcd(8n + 3, 5n + 2) = 1$, for all $n \geq 1$.

Procedure of Euclidean Algorithm

```
procedure gcd(a, b: positive integers)
begin
  r := a mod b
  d := b
  while r > 0 do
    begin
      c := d
      d := r
      r := c mod d
    end
end {gcd(a, b) is d, the last nonzero remainder}
```


Example

- **Example 4.37:** Griffin has two unmarked containers. One container holds 17 ounces and the other holds 55 ounces. Explain how Griffin can use his two containers to measure exactly one ounce.

$$\begin{aligned} 55 &= 3(17) + 4, & 0 < 4 < 17 \\ 17 &= 4(4) + 1, & 0 < 1 < 4 \end{aligned}$$

Therefore $1 = 17 - 4(4) = 17 - 4[44 - 3(17)]$
$= 13(17) - 4(55)$.

Diophantine Equation (1/2)

- **Example 4.38:** On the average, Brian debug a Java program in six minutes, but it takes 10 minutes to debug a C++ program. If he works for 104 minutes and doesn't waste any time, how many programs can be debug in each language.

  We seek integers $x, y \geq 0$, where $6x + 10y = 104$, or $3x + 5y = 52$.

  As $\gcd(3, 5) = 1$, we can write $1 = 3(2) + 5(-1)$, so
  $52 = 3(104) + 5(-52)$
  $= 3(104 - 5k) + 5(-52 + 3k)$, $k \in \mathbf{Z}$.

Diophantine Equation (2/2)

- **Example 4.38 (cont.):**

  Since $0 \leq x = 104 - 5k$ and $0 \leq y = -52 + 3k$, we must have $(52/3) \leq k \leq (104/5)$. So $k = 18, 19, 20$.

  a) $(k = 18)$: $x = 14$, $y = 2$

  b) $(k = 19)$: $x = 9$, $y = 5$

  c) $(k = 20)$: $x = 4$, $y = 8$

- **Theorem 4.8:** If $a, b, c \in \mathbf{Z}^+$, the Diophantine equation $ax + by = c$ has an integer solution $x = x_0$, $y = y_0$ if and only if $\gcd(a, b)$ divides c.

Least Common Multiple (1/2)

- **Definition 4.4:** For $a, b, c \in \mathbf{Z}^+$, c is called a common multiple of a, b if c is a multiple of both a and b. Furthermore, c is the least common multiple of a, b if it is the smallest of all positive integers that are common multiples of a, b. We denote c by $\text{lcm}(a, b)$.

Least Common Multiple (2/2)

- **Theorem 4.9:** Let $a, b, c \in \mathbf{Z}^+$, with $c = \text{lcm}(a, b)$. If d is a common multiple of a and b, then $c|d$.

  Proof: If not, $d = qc + r$, where $0 < r < c$.

  Since $c = \text{lcm}(a, b)$, $c = ma$ for some $m \in \mathbf{Z}^+$.

  Also, $d = na$ for some $n \in \mathbf{Z}^+$.

  Consequently, $na = qma + r \Rightarrow (n - qm)a = r > 0$, and r is a multiple of a.

  In a similar way r could be a multiple of b, so r is a common multiple of a, b.

  But with $0 < r < c$, we contradict the claim that c is the least common multiple of a, b. Hence $c|d$.

GCD and LCM

- **Theorem 4.10:** For all $a, b \in \mathbf{Z}^+$, $ab = \text{lcm}(a, b) \times \gcd(a, b)$.
- **Example 4.40:** By Theorem 4.10, we have

  a) For all $a, b \in \mathbf{Z}^+$, if a, b are relatively prime, then $\text{lcm}(a, b) = ab$.

  b) Since $\gcd(168, 456) = 24$, we find that

$$\text{lcm}(168, 456) = \frac{(168)(456)}{24} = 3{,}192.$$

- **EXERCISES 4.4:** 12, 16

Outline

- The Well-Ordering Principle: Mathematical Induction
- Recursive Definitions
- The Division Algorithm: Prime Numbers
- The Greatest Common Divisor: The Euclidean Algorithm
- ***The Fundamental Theorem of Arithmetic***

Lemmas

- **Lemma 4.2:** $a, b \in \mathbf{Z}^+$ and p is prime, then $p|ab \Rightarrow p|a$ or $p|b$.

  Proof:

  If $p|a$, then we are finished.

  If not, since p is prime, $\gcd(p, a) = 1$, and there exist integers x, y with $px + ay = 1$.

  Then $b = p(bx) + (ab)y$, where $p|p$ and $p|ab$.

  So $p|b$ (**Theorem 4.3** (d) and (e)).
- **Lemma 4.3:** Let $a_i \in \mathbf{Z}^+$ for all $1 \le i \le n$. If p is prime and $p|a_1a_2\ldots a_n$, then $p|a_i$ for some $1 \le i \le n$.

Example

- **Example 4.41:** Show that $\sqrt{2}$ is irrational.

  Proof: If not, we can write $\sqrt{2} = a/b$, where $a, b \in \mathbf{Z}^+$ and $\gcd(a, b) = 1$.

  Then $\sqrt{2} = a/b \Rightarrow 2 = a^2/b^2 \Rightarrow 2b^2 = a^2 \Rightarrow 2|a^2 \Rightarrow \boxed{2|a}$ (why?)

  Also, $2|a \Rightarrow a = 2c$ for some $c \in \mathbf{Z}^+$, so $2b^2 = a^2 = (2c^2) = 4c^2$ and $b^2 = 2c^2$.

  But then $2|b^2 \Rightarrow \boxed{2|b.}$

  Since 2 divides both a and b, it follows that $\gcd(a, b) \ge 2$ (contradiction).

Fundamental Theorem of Arithmetic (1/3)

- **Theorem 4.11:** Every integer $n > 1$ can be written as a product of primes uniquely, up to the order of the primes. (Here a single prime is considered a product of one factor.)

  Proof:

  Existence: If not, let $m > 1$ be the smallest integer not expressible as a product of primes.

  $m = m_1 m_2$ ($\because$ m is composite), and m_1, m_2 can be written as products of primes ($\because$ $1 < m_1, m_2 < m$)

  $\therefore$ m can be expressible as a product of primes.

Fundamental Theorem of Arithmetic (2/3)

- **Theorem 4.11 (cont.):**

  Uniqueness: (Use alternative form of the Principle of Mathematical Induction: **Theorem 4.2**)

  For the integer 2, we have a unique prime factorization, and assuming uniqueness of representation for 3, 4, 5, …, $n - 1$.

  We suppose that $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} = q_1^{t_1} q_2^{t_2} \cdots q_r^{t_r}$, where each p_i, $1 \le i \le k$, and each q_i, $1 \le j \le r$, is a prime. Also $p_1 < p_2 < \ldots < p_k$, and $q_1 < q_2 < \ldots < q_r$, and $s_i > 0$ for all $1 \le i \le k$, $t_j > 0$ for all $1 \le j \le r$.

Fundamental Theorem of Arithmetic (3/3)

- **Theorem 4.11 (cont.):**

  $\because$ $p_1 | n \Rightarrow p_1 | q_1^{t_1} q_2^{t_2} \cdots q_r^{t_r} \Rightarrow p_1 | q_j$ (**Lemma 4.3**)

  $\because$ p_1 and q_j are primes $\Rightarrow p_1 = q_j$

  In fact $j = 1$, for otherwise $q_1 | n \Rightarrow q_1 = p_e$ for some $1 < e \le k$ and $p_1 < p_e = q_1 < q_j = p_1$.

  With $p_1 = q_1$, we find that $n_1 = n/p_1 = p_1^{s_1 - 1} p_2^{s_2} \cdots p_k^{s_k} = q_1^{t_1 - 1} q_2^{t_2} \cdots q_r^{t_r}$.

  Since $n_1 < n$, by the induction hypothesis it follows that $k = r$, $p_i = q_i$ for $1 \le i \le k$, $s_1 - 1 = t_1 - 1$ (so $s_1 = t_1$), and $s_i = t_i$ for $2 \le i \le k$.

  Hence the prime factorization of n is unique.

The Number of Positive Divisors (1/3)

- For $n \in \mathbf{Z}^+$, we want to count the number of positive divisors of n. The number 2 has two positive divisors: 1 and itself. In the case of 4, we find the three positive divisors 1, 2, and 4.
- To determine the result for each $n \in \mathbf{Z}^+$, $n > 1$, we use **Theorem 4.11** and write $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where for each $1 \le i \le k$, p_i is a prime and $e_i > 0$. If $m | n$, then $m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, where $0 \le f_i \le e_i$ for all $1 \le i \le k$. So by the rule of product, the number of positive divisors of n is

$$(e_1 + 1)(e_2 + 1) \ldots (e_k + 1).$$

The Number of Positive Divisors (2/3)

- **Example 4.44:** How many positive divisors do 29,338,848,000 have? How many of the positive divisors are multiples of 360? How many of the positive divisors are perfect squares?

  (i) Since $29{,}338{,}848{,}000 = 2^8 3^5 5^3 7^3 11$, answer = $(8 + 1)(5 + 1)(3 + 1)(3 + 1)(1 + 1) = 1728$ positive divisors.

  (ii) Since $360 = 2^3 2^2 5$, we want to count the integers of the form $2^{t_1} 3^{t_2} 5^{t_3} 7^{t_4} 11^{t_5}$ where $3 \le t_1 \le 8$, $2 \le t_2 \le 5$, $1 \le t_3 \le 3$, $0 \le t_4 \le 3$, and $0 \le t_5 \le 1$. $\therefore$ answer = $[(8 - 3) + 1][(5 - 2) + 1][(3 - 1) + 1][(3 - 0) + 1][(1 - 0) + 1] = 576$.

The Number of Positive Divisors (3/3)

- **Example 4.44 (cont.):**

  (iii) Consider all divisors of the form $2^{s_1} 3^{s_2} 5^{s_3} 7^{s_4} 11^{s_5}$, where each of s_1, s_2, s_3, s_4, s_5 is an even nonnegative integer. Consequently, we have

  5 choices for s_1 – namely, 0, 2, 4, 6, 8;
  3 choices for s_2 – namely, 0, 2, 4;
  2 choices for each of s_3, s_4 – namely, 0, 2;
  1 choices for s_5 – namely, 0.

  $\therefore$ answer = (5)(3)(2)(2)(1) = 60.

Pi-Notation

- We can use the Pi-notation to express the product $x_1 x_2 x_3 x_4 x_5 x_6$ as $\prod_{i=1}^{6} x_i$.
- In general, one can express the product of the $n - m + 1$ terms $x_m, x_{m+1}, x_{m+2}, \ldots, x_n$, where $m, n \in \mathbf{Z}$ and $m \le n$, as $\prod_{i=m}^{n} x_i$.
- **Example:**

$$\prod_{i=3}^{7} x_i = x_3 x_4 x_5 x_6 x_7 = \prod_{j=3}^{7} x_j$$

$$\prod_{i=3}^{6} i = 3 \cdot 4 \cdot 5 \cdot 6 = 6!/2!$$

$$\prod_{i=m}^{n} i = m(m+1)(m+2)\cdots(n-1)(n) = n!/(m-1)!$$

$$\prod_{i=7}^{11} x_i = x_7 x_8 x_9 x_{10} x_{11} = \prod_{j=0}^{4} x_{7+j} = \prod_{j=0}^{4} x_{11-j}$$

GCD and LCM

- **Example 4.45:** If $m, n \in \mathbf{Z}^+$, let $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ and $n = p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$, with each p_i prime and $0 \le e_i$ and $0 \le f_i$ for all $1 \le i \le t$. Then if $a_i = \min\{e_i, f_i\}$ and $b_i = \max\{e_i, f_i\}$, for all $1 \le i \le t$, we have

$$\gcd(m, n) = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t} = \prod_{i=1}^{t} p_i^{a_i}$$

$$\operatorname{lcm}(m, n) = p_1^{b_1} p_2^{b_2} \cdots p_t^{b_t} = \prod_{i=1}^{t} p_i^{b_i}$$

Perfect Square (1/2)

- **Example 4.46:** Can we find three consecutive positive integers whose product is a perfect square – that is, do there exist $m, n \in \mathbf{Z}^+$ with $m(m+1)(m+2) = n^2$?

  Proof: Suppose such m, n do exist.

  Use the fact that $\gcd(m, m+1) = 1 = \gcd(m+1, m+2)$

  For any prime p, if $p|(m+1)$ then $p \nmid m$ and $p \nmid m+2$, and $p|n^2$.

  $\because$ n^2 is a perfect square $\therefore$ $m+1$ is also a perfect square.

Perfect Square (2/2)

- **Example 4.46 (cont.):**

  $\therefore$ $m(m+2)$ is also a perfect square.

  $\because$ $m^2 < m^2 + 2m = m(m+2) < m^2 + 2m + 1 = (m+1)^2$

  $\therefore$ $m(m+2)$ cannot be a perfect square.

➡ So, we conclude that there are no three consecutive positive integers whose product is a perfect square.

Homework Assignment #4

- **EXERCISES 4.1**
  18, 24
- **EXERCISES 4.2**
  12, 16
- **EXERCISES 4.3**
  10, 12, 18
- **EXERCISE 4.4**
  12, 16
- **EXERCISE 4.5**
  8