Lamé’s Theorem: Let \( a \) and \( b \) be positive integers with \( a \geq b \). Then the number of divisions used by the Euclidian algorithm to find \( \gcd(a, b) \) is less than or equal to five times the number of decimal digits in \( b \).

**Proof:** in book.

- As a consequence of Lamé’s Theorem, \( O(\log \, b) \) divisions are used by the Euclidian algorithm to find \( \gcd(a, b) \) whenever \( a > b \).

---

**Recursively Defined Sets and Structures**

*Recursive definitions* of sets have two parts:
- The *basis step* specifies an initial collection of elements.
- The *recursive step* gives the rules for forming new elements in the set from those already known to be in the set.

- Sometimes the recursive definition has an *exclusion rule*, which specifies that the set contains nothing other than those elements specified in the basis step and generated by applications of the rules in the recursive step.
- We will always assume that the exclusion rule holds, even if it is not explicitly mentioned.
- We will later develop a form of induction, called *structural induction*, to prove results about recursively defined sets.

**Example:** Subset of Integers \( S \):
- **Basis step:** \( 3 \in S \).
- **Recursive step:** If \( x \in S \) and \( y \in S \), then \( x + y \) is in \( S \).
- Initially \( 3 \) is in \( S \), then \( 3 + 3 = 6 \), then \( 3 + 6 = 9 \), etc.

**Example:** The natural numbers \( \mathbb{N} \).
- **Basis step:** \( 0 \in \mathbb{N} \).
- **Recursive step:** If \( n \) is in \( \mathbb{N} \), then \( n + 1 \) is in \( \mathbb{N} \).
- Initially \( 0 \) is in \( \mathbb{N} \), then \( 0 + 1 = 1 \), then \( 1 + 1 = 2 \), etc.

**Strings**

**Definition:** The set \( \Sigma^* \) of *strings* over the alphabet \( \Sigma \):
- **Basis step:** \( \lambda \in \Sigma^* \) (\( \lambda \) is the empty string)
- **Recursive step:** If \( w \) is in \( \Sigma^* \) and \( x \) is in \( \Sigma \), then \( wx \in \Sigma^* \).

**Example:** If \( \Sigma = \{0, 1\} \), the strings in \( \Sigma^* \) are the set of all bit strings, \( \lambda, 0, 1, 00, 01, 10, 11, \) etc.

**Example:** If \( \Sigma = \{a, b\} \), show that \( aab \) is in \( \Sigma^* \).
- Since \( \lambda \in \Sigma^* \) and \( a \in \Sigma \), \( a \in \Sigma^* \).
- Since \( a \in \Sigma^* \) and \( a \in \Sigma \), \( aa \in \Sigma^* \).
- Since \( aa \in \Sigma^* \) and \( b \in \Sigma \), \( aab \in \Sigma^* \).
String Concatenation

**Definition:** Two strings can be combined via the operation of *concatenation*. Let \( \Sigma \) be a set of symbols and \( \Sigma^* \) be the set of strings formed from the symbols in \( \Sigma \). We can define the concatenation of two strings, denoted by \( \cdot \), recursively as follows.

**BASIS STEP:** If \( w \in \Sigma^* \), then \( w \cdot \lambda = w \).

**RECURSIVE STEP:** If \( w_1 \in \Sigma^* \) and \( w_2 \in \Sigma^* \) and \( x \in \Sigma \), then \( w_1 \cdot (w_2 x) = (w_1 \cdot w_2) x \).

- Often \( w_1 \cdot w_2 \) is written as \( w_1 w_2 \).
- If \( w_1 = \text{abra} \) and \( w_2 = \text{cadabra} \), the concatenation \( w_1 w_2 = \text{abracadabra} \).

Length of a String

**Example:** Give a recursive definition of \( l(w) \), the length of the string \( w \).

**Solution:** The length of a string can be recursively defined by:

\[
 l(w) = 0; \\
 l(wx) = l(w) + 1 \text{ if } w \in \Sigma^* \text{ and } x \in \Sigma. 
\]

Balanced Parentheses

**Example:** Give a recursive definition of the set of balanced parentheses \( P \).

**Solution:**

- **BASIS STEP:** \( () \in P \)
- **RECURSIVE STEP:** If \( w \in P \), then \( () w \in P \), \( (w) \in P \) and \( w () \in P \).
- Show that \( (()()) \) is in \( P \).
- Why is \( ))(\) not in \( P \)?

Well-Formed Formulae in Propositional Logic

**Definition:** The set of *well-formed formulae* in propositional logic involving \( T, F \), propositional variables, and operators from the set \( \{ \neg, \land, \lor, \rightarrow, \leftrightarrow \} \).

**BASIS STEP:** \( T, F, \) and \( s \), where \( s \) is a propositional variable, are well-formed formulae.

**RECURSIVE STEP:** If \( E \) and \( F \) are well formed formulae, then \( (\neg E) \), \( (E \land F) \), \( (E \lor F) \), \( (E \rightarrow F) \), \( (E \leftrightarrow F) \), are well-formed formulae.

**Examples:** \( ((p \lor q) \rightarrow (q \land F)) \) is a well-formed formula.
\[ pq \land \] is not a well formed formula.
Rooted Trees

**Definition:** The set of *rooted trees*, where a rooted tree consists of a set of vertices containing a distinguished vertex called the *root*, and edges connecting these vertices, can be defined recursively by these steps:

**BASIS STEP:** A single vertex $r$ is a rooted tree.

**RECURSIVE STEP:** Suppose that $T_1, T_2, \ldots, T_n$ are disjoint rooted trees with roots $r_1, r_2, \ldots, r_n$, respectively. Then the graph formed by starting with a root $r$, which is not in any of the rooted trees $T_1, T_2, \ldots, T_n$, and adding an edge from $r$ to each of the vertices $r_1, r_2, \ldots, r_n$, is also a rooted tree.

Building Up Rooted Trees

- Trees are studied extensively in Chapter 11.
- Next we look at a special type of tree, the full binary tree.

How do you construct this rooted tree recursively?

Full Binary Trees

**Definition:** The set of *full binary trees* can be defined recursively by these steps.

**BASIS STEP:** There is a full binary tree consisting of only a single vertex $r$.

**RECURSIVE STEP:** If $T_1$ and $T_2$ are disjoint full binary trees, there is a full binary tree, denoted by $T_1 \cdot T_2$, consisting of a root $r$ together with edges connecting the root to each of the roots of the left subtree $T_1$ and the right subtree $T_2$. 
Building Up Full Binary Trees

What can you say about the nonleaf nodes in a full binary tree?

Induction and Recursively Defined Sets

Example: Show that the set $S$ defined by specifying that $3 \in S$ and that if $x \in S$ and $y \in S$, then $x + y$ is in $S$, is the set of all positive integers that are multiples of 3.

Solution: Let $A$ be the set of all positive integers divisible by 3. To prove that $A = S$, show that $A$ is a subset of $S$ and $S$ is a subset of $A$.

- $A \subseteq S$: Let $P(n)$ be the statement that $3n$ belongs to $S$.
  BASIS STEP: $3 \cdot 1 = 3 \in S$, by the first part of recursive definition.
  INDUCTIVE STEP: Assume $P(k)$ is true.
  By the second part of the recursive definition, if $3k \in S$, then since $3 \in S$, $3k + 3 = 3(k + 1) \in S$.
  Hence, $P(k + 1)$ is true.

- $S \subseteq A$:
  BASIS STEP: $3 \in S$ by the first part of recursive definition, and $3 = 3 \cdot 1$.
  INDUCTIVE STEP: The second part of the recursive definition adds $x + y$ to $S$, if both $x$ and $y$ are in $S$.
  If $x$ and $y$ are both in $A$, then both $x$ and $y$ are divisible by 3.
  By part (i) of Theorem 1 of Section 4.1, it follows that $x + y$ is divisible by 3.

Structural Induction

We used mathematical induction to prove a result about a recursively defined set. Next, we study a more direct form induction for proving results about recursively defined sets.

Definition: To prove a property of the elements of a recursively defined set, we use *structural induction*.

BASIS STEP: Show that the result holds for all elements specified in the basis step of the recursive definition.

RECURSIVE STEP: Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

- The validity of structural induction can be shown to follow from the principle of mathematical induction.
Full Binary Trees

**Definition:** The height $h(T)$ of a full binary tree $T$ is defined recursively as follows:
- **Basis Step:** The height of a full binary tree $T$ consisting of only a root $r$ is $0$.
- **Recursive Step:** If $T_1$ and $T_2$ are full binary trees, then the full binary tree $T = T_1 \cdot T_2$ has height $h(T) = 1 + \max(h(T_1), h(T_2))$.

• The number of vertices $n(T)$ of a full binary tree $T$ satisfies the following recursive formula:
  - **Basis Step:** The number of vertices of a full binary tree $T$ consisting of only a root is $1$.
  - **Recursive Step:** If $T_1$ and $T_2$ are full binary trees, then the full binary tree $T = T_1 \cdot T_2$ has the number of vertices $n(T) = 1 + n(T_1) + n(T_2)$.

**Theorem:** If $T$ is a full binary tree, then $n(T) \leq 2^{h(T)+1} - 1$.

**Proof:** Use structural induction.
- **Basis Step:** The result holds for a full binary tree consisting only of a root, $n(T) = 1$ and $h(T) = 0$. Hence, $n(T) = 1 \leq 2^0 - 1 = 1$.
- **Recursive Step:** Assume $n(T_1) \leq 2^{h(T_1)+1} - 1$ and also $n(T_2) \leq 2^{h(T_2)+1} - 1$ whenever $T_1$ and $T_2$ are full binary trees.

\[
n(T) = 1 + n(T_1) + n(T_2) \quad \text{(by recursive formula of } n(T))
\]

Full Binary Trees

**Definition:** The height $h(T)$ of a full binary tree $T$ is defined recursively as follows:
- **Basis Step:** The height of a full binary tree $T$ consisting of only a root $r$ is $h(T) = 0$.
- **Recursive Step:** If $T_1$ and $T_2$ are full binary trees, then the full binary tree $T = T_1 \cdot T_2$ has height $h(T) = 1 + \max(h(T_1), h(T_2))$.

**Theorem:** If $T$ is a full binary tree, then $n(T) \leq 2^{h(T)+1} - 1$.

**Proof:** Use structural induction.
- **Basis Step:** The result holds for a full binary tree consisting only of a root, $n(T) = 1$ and $h(T) = 0$. Hence, $n(T) = 1 \leq 2^0 - 1 = 1$.
- **Recursive Step:** Assume $n(T_1) \leq 2^{h(T_1)+1} - 1$ and also $n(T_2) \leq 2^{h(T_2)+1} - 1$ whenever $T_1$ and $T_2$ are full binary trees.

\[
n(T) = 1 + n(T_1) + n(T_2) \quad \text{(by recursive formula of } n(T))
\]

\[
\leq 1 + (2^{h(T_1)+1} - 1) + (2^{h(T_2)+1} - 1) \quad \text{(by inductive hypothesis)}
\]

\[
\leq 2 \cdot \max(2^{h(T_1)+1}, 2^{h(T_2)+1}) - 1
\]

\[
= 2 \cdot 2^{\max(h(T_1), h(T_2))+1} - 1
\]

\[
= 2^{h(T)+1} - 1 \quad \text{(by recursive definition of } h(T))
\]
Generalized Induction

- **Generalized induction** is used to prove results about sets other than the integers that have the well-ordering property. (explored in more detail in Chapter 9)
- For example, consider an ordering on \( \mathbb{N} \times \mathbb{N} \), ordered pairs of nonnegative integers. Specify that \((x_1, y_1)\) is less than or equal to \((x_2, y_2)\) if either \(x_1 < x_2\), or \(x_1 = x_2\) and \(y_1 < y_2\). This is called the lexicographic ordering.
- Strings are also commonly ordered by a lexicographic ordering.
- The next example uses generalized induction to prove a result about ordered pairs from \( \mathbb{N} \times \mathbb{N} \).

**Example**: Suppose that \( a_{m,n} \) is defined for \((m,n) \in \mathbb{N} \times \mathbb{N} \) by

\[
a_{0,0} = 0 \quad \text{and} \\
a_{m,n} = \begin{cases} 
  a_{m-1,n} + 1 & \text{if } n = 0 \text{ and } m > 0 \\
  a_{m,n-1} + n & \text{if } n > 0 
\end{cases}
\]

Show that \( a_{m,n} = m + n(n + 1)/2 \) is defined for all \((m,n) \in \mathbb{N} \times \mathbb{N} \).

**Solution**: Use generalized induction.

**Basis Step**: \( a_{0,0} = 0 = 0 + (0 \cdot 1)/2 \)

**Inductive Step**: Assume that \( a_{m',n'} = m' + n'(n' + 1)/2 \) whenever \((m',n')\) is less than \((m,n)\) in the lexicographic ordering of \( \mathbb{N} \times \mathbb{N} \).

- If \( n = 0 \), by the inductive hypothesis we can conclude
  \[a_{m,n} = a_{m-1,n} + 1 = m - 1 + n(n + 1)/2 + 1 = m + n(n + 1)/2.\]
- If \( n > 0 \), by the inductive hypothesis we can conclude
  \[a_{m,n} = a_{m,n-1} + 1 = m + n(n - 1)/2 + n = m + n(n + 1)/2.\]