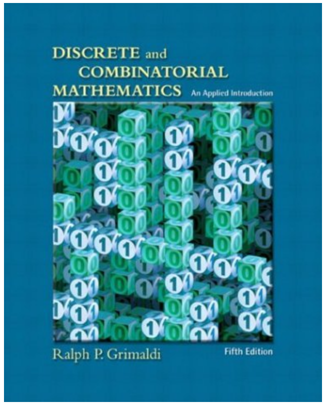
Discrete Mathematics
-- *Chapter 4: Properties of the Integers: Mathematical Induction*



Hung-Yu Kao (高宏宇)
Department of Computer Science and Information Engineering,
National Cheng Kung University

Outline

- 4.1 The Well-Ordering Principle: Mathematical Induction
- 4.2 Recursive Definitions
- 4.3 The Division Algorithm: Prime Numbers
- 4.4 The Greatest Common Divisor: The Euclidean Algorithm
- 4.5 The fundamental Theorem of Arithmetic

自然數 *(p.243)*

- 自然數要適合五點(**Peano axioms)**：
  - 有一起始自然數 0。
  - 任一自然數 a 必有**後繼(successor)**，記作 a+1。
  - 0 並非任何自然數的後繼。
  - 不同的自然數有不同的後繼。
  - （數學歸納公設）有一與自然數有關的命題。設此命題對 0 成立，而當對任一自然數成立時，則對其後繼亦成立，則此命題對所有自然數皆成立。

4.1 The Well-Ordering Principle: Mathematical Induction

- **The Well-Ordering Principle**: Every nonempty subset of $\mathbf{Z}^+$ contains a **smallest** element.
  ($\mathbf{Z}^+ = \{x \in \mathbf{Z} \mid x > 0\} = \{x \in \mathbf{Z} \mid x \geq 1\}$)
  $\mathbf{Z}^+$ is well ordered
- **The Principle of Mathematical Induction**: Let $S(n)$ denote an open mathematical statement that involves one or more occurrences of the variable n, which represents a positive integer.
  a) If $S(1)$ is true; and (basis step)
  b) If whenever $S(k)$ is true, then $S(k+1)$ is true. (inductive step)

  then $S(n)$ is true for all $n \in \mathbf{Z}^+$
- Using quantifiers

$$\boxed{[S(n_0) \wedge [\forall k \geq n_0 [S(k) \Rightarrow S(k+1)]]] \Rightarrow \forall n \geq n_0 \; S(n)}$$

4.1 The Well-Ordering Principle: Mathematical Induction

Inductive step

Basic step

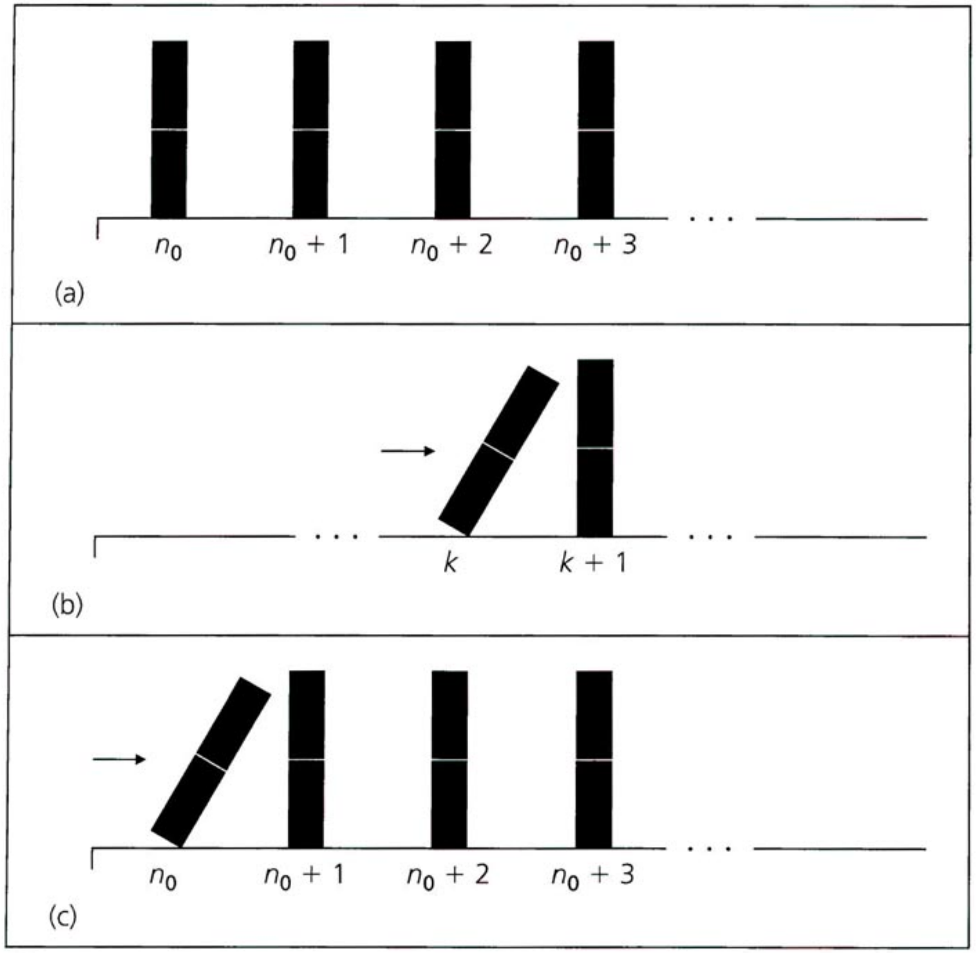


Figure 4.1

$P(n_0)$
$P(n_0+1)$
$P(n_0+2)$
.
.
.

Why Induction Works

- More rigorously, the validity of a proof by mathematical induction relies on the well-ordering of $\mathbf{Z}^+$.
- Let S be a statement for which we have proven that S(1) holds and for all $n \in \mathbf{Z}^+$ we have $S(n) \Rightarrow S(n+1)$. Claim: S(n) holds for all $n \in \mathbf{Z}^+$

- **Proof by contradiction**: Define the set $F \subseteq \mathbf{Z}^+$ of values for which S does not hold: $F = \{ m \mid S(m) \text{ does not hold} \}$.
  - If F is non-empty, then F **must have a smallest element** (well-ordering of $\mathbf{Z}^+$), let this number be z with $\neg S(z)$. Because we know that S(1), it must hold that $z>1$. Because z is the smallest value, it must hold that $S(z-1)$, which contradicts our proof for all $n \in \mathbf{Z}^+$: $S(n) \Rightarrow S(n+1)$.
  - Contradiction: F has to be empty: S holds for all $\mathbf{Z}^+$.

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.1** : For any $n \in \mathbf{Z}^+, \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$
  - Proof

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

(i) $S(1) : \sum_{i=1}^{1} i = 1 = \frac{1 \times (1+1)}{2}$

(ii) Assume $S(k)$ is true, i.e., $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

(iii) Then $S(k+1) : \sum_{i=1}^{k+1} i = 1 + 2 + 3 + \cdots + k + (k+1)$

$$= \left(\sum_{i=1}^{1} i\right) + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

$$= \frac{(k+1)(k+2)}{2}$$

$$\boxed{\text{try } n \in \mathbf{Z}^+, \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n^2+n+2}{4}}$$

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.3** : Among the 900 three-digit integers (100 to 999), 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.
  - Solution

    The typical palindrome: $aba = 100a + 10b + a = 101a + 10b$

$$\sum_{a=1}^{9}\left(\sum_{b=0}^{9} aba\right) = \sum_{a=1}^{9}\sum_{b=0}^{9}(101a + 10b)$$

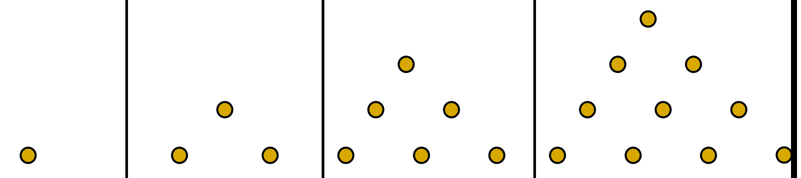
$$= \sum_{a=1}^{9}\left[10(101a) + 10\sum_{b=0}^{9} b\right] = \sum_{a=1}^{9}[1010a + 10\cdot 45]$$

$$= 1010\sum_{a=1}^{9} a + 9\cdot 450 = 49{,}500$$

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.5**
  - For triangular number t_i=1+2 +…+i= $i(i$+1)/2
  - We want a formula for the sum of the first n triangular numbers.
  - Proof

$t_1 = 1 = \frac{1\cdot 2}{2}$	$t_2 = 1 + 2$ $= 3 = \frac{2\cdot 3}{2}$	$t_3 = 1 + 2 + 3$ $= 6 = \frac{3\cdot 4}{2}$	$t_4 = 1 + 2 + 3 + 4$ $= 10 = \frac{4\cdot 5}{2}$



$$\sum_{i=1}^{n} t_i = \sum_{i=1}^{n} \frac{i(i+1)}{2} = \frac{1}{2}\sum_{i=1}^{n}(i^2 + i) = \frac{1}{2}\left[\frac{n(n+1)(2n+1)}{6}\right] + \frac{1}{2}\left[\frac{n(n+1)}{2}\right]$$

Ex 4.4 prove it

$$= \frac{n(n+1)(n+2)}{6}$$

$$\therefore t_1 + t_2 + \ldots + t_{100} = \frac{100(101)(102)}{6} = 171{,}700$$

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.8**
  - For $n \geq 6,\ 4n < (n^2 - 7)$.
  - Solution

n	$4n$	n^2-7	n	$4n$	n^2-7
1	4	-6	5	20	18
2	8	-3	6	24	29
3	12	2	7	28	42
4	16	9	8	32	57

2*6+1=13 ≥4

$$S(k): 4k < (k^2 - 7),\ k \geq 6$$

$$S(k+1): 4(k+1) = 4k + 4 < (k^2 - 7) + 4 < (k^2 - 7) + \boxed{(2k+1)}$$

$$\Rightarrow 4(k+1) < (k^2 - 7) + (2k+1) = (k+1)^2 - 7$$

$\therefore S(n)$ is true.

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.9** : Harmonic numbers $H_1 = 1, H_2 = 1 + \frac{1}{2}, \cdots, H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$

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

- Proof

Verify $S(1): \sum_{j=1}^{1} H_j = H_1 = 1 = (1+1)H_1 - 1$

Assume $S(k)$ true : $\sum_{j=1}^{k} H_j = (k+1)H_k - k$

Verify $S(k+1): \sum_{j=1}^{k+1} H_j = \sum_{j=1}^{k} H_j + H_{k+1} = [(k+1)H_k - k] + H_{k+1}$

$$= (\mathrm{k}+1)H_k - k + H_{k+1}$$

$$= (\mathrm{k}+1)[H_{k+1} - \frac{1}{k+1}] - k + H_{k+1}$$

$$= (\mathrm{k}+2)H_{k+1} - (k+1)$$

$\therefore S(n)$ is true.

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.10** :
  - The elements of A_n are listed in ascending order, and $|A_n| = 2^n$.
  - To determine whether $r \in A_n$, we must compare r with no more than $n+1$ elements in A_n.
  - Proof

Verify $S(1): A_1 = \{a_1, a_2\}, a_1 < a_2 \therefore$ at most 2 comparisons

Verify $S(2): A_2 = \{b_1, b_2, c_1, c_2\} = B_1 \cup C_1, b_1 < b_2 < c_1 < c_2, B_1 = \{b_1, b_2\}, C_1 = \{c_1, c_2\}$

(i) compare r with b_2

(ii) $r \in B_1$, or $r \in C_1, |B_1| = |C_1| = 2 \therefore$ at most 2 comparisons

(iii) $\therefore$ at most $2+1 = n+1$ comparisons

Assume $S(k)$ true :

Verify $S(k+1)$: Let $A_{k+1} = B_k \cup C_k = \{b_1, b_2, \cdots, b_2k, c_1, c_2, \cdots, c_2k\}$,

$$b_1 < b_2 < \cdots < b_2k < c_1 < c_2 < \cdots < c_2k$$

The Well-Ordering Principle: Mathematical Induction

- Mathematical induction plays a major role in programming verification.
- **Ex 4.11** :
  - The pseudocode program segment is supposed to produce the answer xy^n.
  - Proof

```
while n≠ 0 do
  begin
    x := x * y
    n := n - 1
  end
answer := x
```

Verify $S(0)$: answer $= x = xy^0$

Assume $S(k)$ true: answer $= xy^k$

Verify $S(k+1)$: when $n = k+1$, the program reach the the top of the 'while' loop for the first time, the loop instructions are executed and return to the top of the 'while' loop again, now we find

- $x_1 = xy$
- $n = (k+1) - 1 = k$

And the 'while' loop will continue with x_1, y and $n = k$

$\therefore$ The final answer $= x_1 y^k = (xy)y^k = xy^{k+1}$

$\therefore S(n)$ is true.

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.13** :
  - Show that for all $n \geq 14$ we can express n using only 3's and 8's as summands. (e.g., 14 = 3 + 3+ 8)
  - Proof

Assume $S(k)$ true:

Verify $S(k+1)$:

While $n = k$

case (i) at least one 8 appears in the sum, replace 8 with three 3's for $n = k+1$

case (ii) no 8 appears in the sum, $\because \geq 14, \therefore$ the sum have at least five 3's,

replace five 3's with two 8's for $n = k+1$

$\therefore S(k) \Rightarrow S(k+1)$

Fibonacci Sequence

- Consider the sequence 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89,… which is defined by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$
- Clearly this sequence $F_1, F_2, \ldots$ will grow, but how fast?
- **Conjecture**: $F_n \geq (3/2)^n$ for all $n>10$
- **Proof by induction**:

Base case: Indeed $F_{11} = 89 \geq (3/2)^{11} = 86.49756\ldots$

Other base case: also $F_{12} = 144 \geq (3/2)^{12} = 129.746338\ldots$

- Inductive step for $n>10$:

Assume $F_n \geq (3/2)^n$ and $F_{n+1} \geq (3/2)^{n+1}$, then indeed

- $F_{n+2} = F_n + F_{n+1} \geq (3/2)^n + (3/2)^{n+1} = (3/2)^n(1 + (3/2))$
- $= (3/2)^n(5/2) \geq (3/2)^n (9/4) = (3/2)^{n+2}$
- By induction on n, the conjecture holds.

Other Induction Proofs

- We just saw a different kind of proof by induction where the inductive step is $\forall n>10$: [P(n), P(n+1) $\Rightarrow$ P(n+2)]
  This time the basis step is proving P(11) *and* P(12).

- There are many variations of proof by induction:
  Strong/ Complete induction: Here the inductive step is:
  Assume all of P(1),…,P(n), then prove P(n+1).
  The basis step is P(1) for this alternative form of induction.

Fibonacci Numbers

- The sequence 1,1,2,3,5,8,13,21,34,… defined by $F_{n+2}= F_n+F_{n+1}$ is the famous **Fibonacci sequence**.

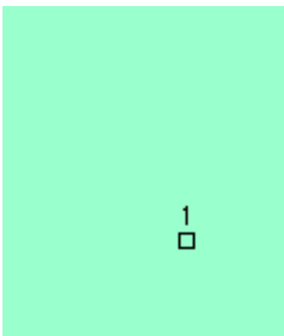
- A closed expression of F_n is

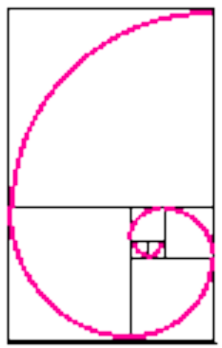
$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

- For large n, it grows like $F_n \approx 0.447214 \times 1.61803^n$.
- This $(1+\sqrt{5})/2 \approx 1.61803$ is the **Golden Ratio**.
- Fn/Fn+1 ≈ 0.618

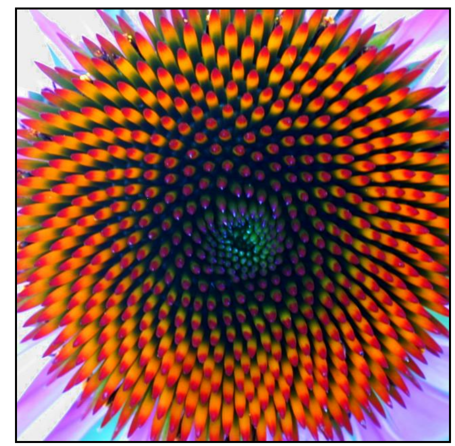
Fibonacci in Nature

- Fibonacci numbers often occur in the natural world.
- Shape of shells:





Number of petals on flowers:



http://www.research.att.com/~njas/sequences/index.html

The Well-Ordering Principle: Mathematical Induction

- Theorem 4.2: The Principle of Mathematical Induction – Alternative Form: (or the **Principle of Strong Mathematical Induction**)
  - Let $S(n)$ denote an open mathematical statement that involves one or more occurrences of the variable n, which represents a positive integer.
    a) If $S(n_0)$, $S(n_0+1)$, …, $S(n_1-1)$, and $S(n_1)$ are true *Basic step*
    b) If whenever $S(n_0)$, $S(n_0+1)$, …, $S(k-1)$, and $S(k)$ are true for some $k \in \mathbf{Z}^+$, where $k \geq n_1$, then $S(k+1)$ is also true *inductive step*

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

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.14** :
  - Show that for all $n \geq 14$, n can be written as a sum of only 3's and 8's. (e.g., 14 = 3+3+8, 15 = 3+3+3+3+3, 16 = 8+8)
  - Proof

Verify $S(14), S(15)$, and $S(16)$ are true.

Assume $S(14), S(15), \cdots, S(k-2), S(k-1)$ and $S(k)$ are true, where $k \geq 16$

Verify $S(k+1)$:

$\because k+1 = (k-2) + \underline{3}$, and $14 \leq k-2 \leq k$, $S(k-2)$ is true

$\therefore S(k+1)$ is true

14 15 16 17 18 19 20 21 22 …

The Well-Ordering Principle: Mathematical Induction

- **Ex 4.15** :
  - Show that $a_n \le 3^n$, where

$$\begin{cases} a_0 = 1, a_1 = 2, a_2 = 3, \text{ and} \\ a_n = a_{n-1} + a_{n-2} + a_{n-3}, \text{ for all } n \in \mathbf{Z}^+ \text{ where } n \ge 3 \end{cases}$$

  - Proof

$$\text{(i) } a_0 = 1 = 3^0 \le 3^0$$

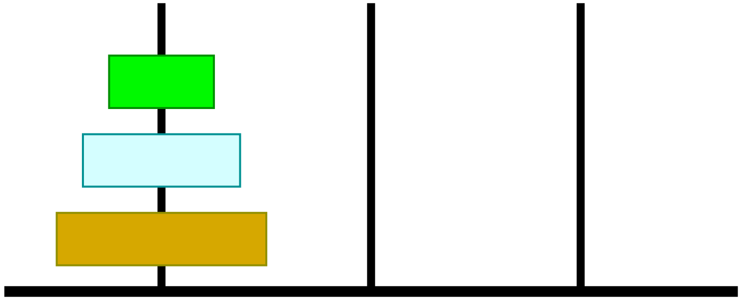
$$a_1 = 2 \le 3 = 3^1$$

$$a_2 = 3 \le 9 = 3^2$$

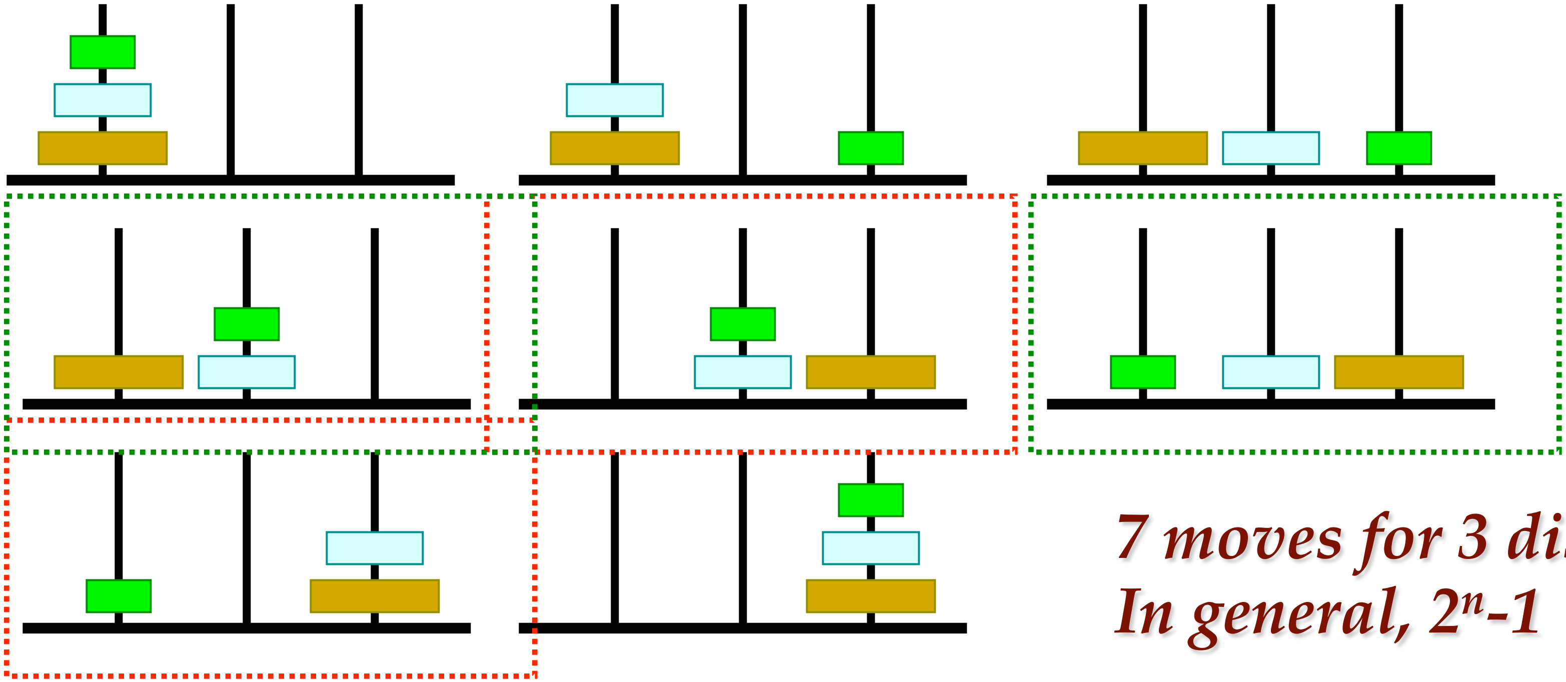
$$\begin{aligned} \text{(ii) } a_{k+1} &= a_k + a_{k-1} + a_{k-2} \\ &\le 3^k + 3^{k-1} + 3^{k-2} \\ &\le 3^k + 3^k + 3^k = 3(3^k) = 3^{k+1} \end{aligned}$$

Induction, another example

- **Towers of Hanoi**: (1883)
  - We have three poles and n golden disks
  - the disks are only allowed in pyramid shape
    - no big disks on top of smaller ones
- How to move the disks from one pole to another?
- How many moves are requires?
- Call this number M(n).
  Note M(1)=1 and M(2)=3
  What about M(3)?



Inductive, Recursive



7 moves for 3 disks

In general, 2^n-1

Making a Conjecture

- To prove something by induction, you need a conjecture about the general case M(n).

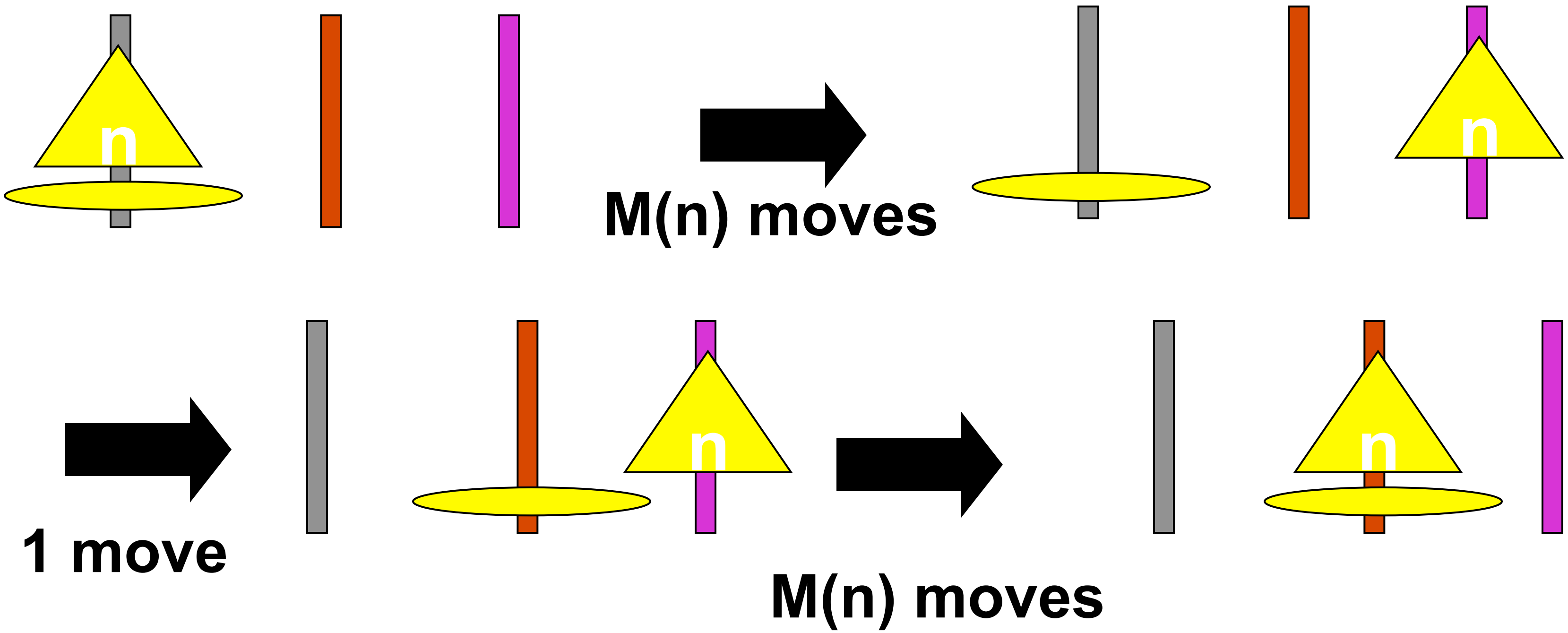
- Here we have: M(1)=1, M(2)=3, M(3)=7,…
- Obvious conjecture… $M(n) = 2^n – 1$ for all $n > 0$

- Clearly, the basis step M(1)=1 holds.

- Feeling for general n case: Each additional disk (almost) doubles the number of moves:
M(n+1) consists of two M(n) cases…

Inductive Step

How to move n+1 disks, using an n-disk 'subroutine'?

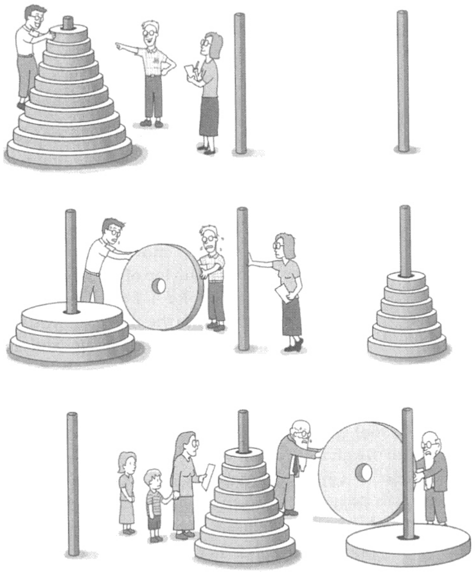


In sum: M(n+1) = 2 M(n)+1

Proof of ToH

- We just saw that for all n, we have $M(n+1) = 2M(n)+1$. This enables our proof of the conjecture $M(n)=2^n-1$.
- Proof: Basis step: $M(1) = 2^1-1 = 1$ holds.
- Assume that $M(n)=2^n-1$ holds. Then, for next $n+1$:
- $M(n+1) = 2\ M(n) + 1 = 2(2^n-1) + 1 = 2^{n+1} - 1$.
- Hence it holds for n+1. End of proof by induction on n.

With n=64 golden disks, and one move per second, this amounts to almost 600,000,000,000 years of work.



How to Prove Inductively

- **General strategy:**
  1. Clarify on which variable you're going to do the induction
  2. Calculate some small cases n=1,2,3,…(Come up with your conjecture)
  3. Make clear what the induction step $n \rightarrow n+1$ is
  4. Prove the basis step, prove the inductive step, and say that you proved it.

Induction in CS

- Inductive proofs play an important role in computer science because of their similarity with **recursive algorithms**.

- Analyzing recursive algorithms often require the use of recurrent equations, which require inductive proofs.

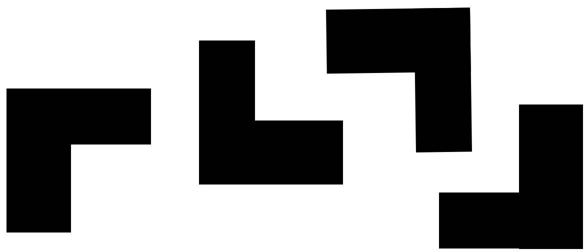
Structural Induction

- The method of induction can also be applied to structures other than integers, like graphs, matrices, trees, sequences and so on.
- The crucial property that must hold is the **well-ordered principle**: there has to be a notion of size such that all objects have a finite size, and each set of objects must have a smallest object.
- **Examples**: vertex size of graphs, dimension of matrices, depth of trees, length of sequences and so on.

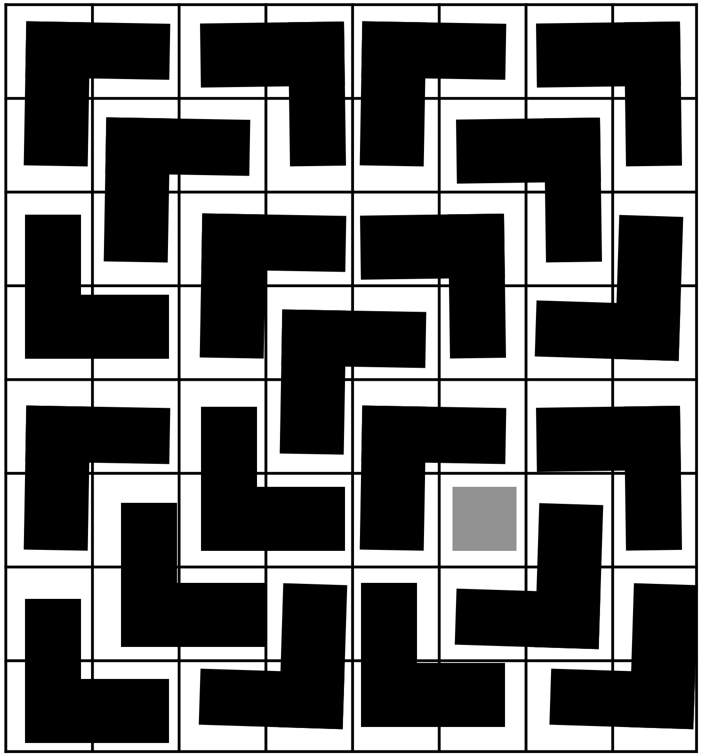
L-Tiling an $2^n \times 2^n$ Square

Take a $2^n \times 2^n$ square with one tile missing

Can you tile it with L-shapes?

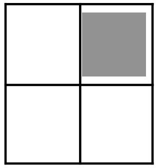


Theorem:
Yes, you can for all n.



Example for 8×8:

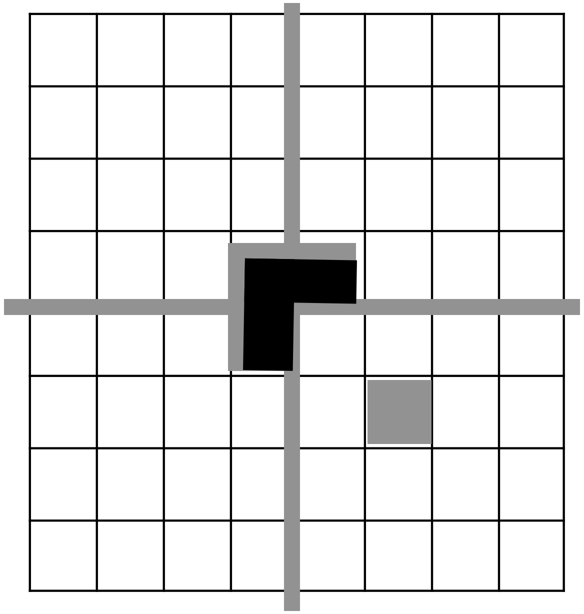
Proving L-Tiling



Basis step of 2×2 squares is easy.

Inductive step: Assuming that $2^n \times 2^n$ tiling is possible, tile a $2^{n+1} \times 2^{n+1}$ square by looking at 4 sub-squares:

Put the 3 holes in the middle:



Put an L in the middle, and tile the sub-squares using the assumption.

Proof by induction on n.

This is a constructive proof.

4.2 Recursive Definitions

- **Ex 4.19** : Fibonacci numbers
  1) $F_0 = 0; F_1 = 1;$
  2) $F_n = F_{n\text{-}1} + F_{n\text{-}2},$ for all $n \in \mathbf{Z}^+$ where $n \geq 2$

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

- Proof

basis step, $F_0^2 + F_1^2 = 1*1$

Assume $\sum_{i=0}^{k} F_i^2 = F_k \times F_{k+1}$

$$\text{Then } \sum_{i=0}^{k+1} F_i^2 = \sum_{i=0}^{k} F_i^2 + F_{k+1}^2$$

$$= F_k \times F_{k+1} + F_{k+1}^2$$

$$= F_{k+1} \times (F_k + F_{k+1})$$

$$= F_{k+1} \times F_{k+2}$$

- $L_n = F_{n-1} + F_{n+1}$
- $L_n^2 = 5F_n^2 + 4(-1)^n$
- $F_{2n} = L_n F_n$
- $F_{n+k} + (-1)^k F_{n-k} = L_k F_n$
- $F_n = \dfrac{L_{n-1} + L_{n+1}}{5}$

Recursive Definitions

- **Ex 4.20** : Lucas numbers
  1) $L_0 = 2;\ L_1 = 1;$
  2) $L_n = L_{n-1} + L_{n-2},$ for all $n \in \mathbf{Z}^+$ where $n \geq 2$

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

Proof :

basis step, $L_1 = 1 = 0 + 1 = F_0 + F_2,\ L_2 = 3 = 1 + 2 = F_1 + F_3$

Assume $L_n = F_{n-1} + F_{n+1}$ for $n = 1,2,3,\ldots,k-1,k$, where $k \geq 2$

Then $L_{k+1} = L_k + L_{k-1} = (F_{k-1} + F_{k+1}) + (F_{k-2} + F_k)$

$$= (F_{k-1} + F_{k-2}) + (F_{k+1} + F_k)$$

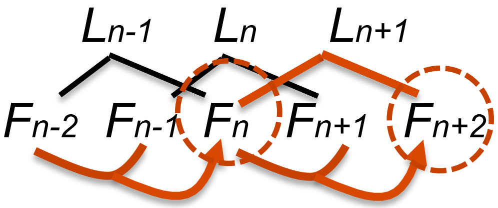
$$= F_k + F_{k+2}$$

$$= F_{(k+1)-1} + F_{(k+1)+1}$$

Table 4.2

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

Édouard Lucas (1842~1891)



Recursive Definitions

- **Ex 4.21** : Eulerian numbers

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

$$a_{0,0} = 1, \qquad a_{m,k} = 0, k \ge m, \qquad a_{m,k} = 0, k < 0,$$

$$\textstyle\sum_{k=0}^{m-1} a_{m,k} = m!$$

		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!

- Proof

Induction on m

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

4.3 The Division Algorithm: Prime Numbers

- Definition 4.1: If $a, b \in Z$ and $b \neq 0$, we say <u>*b divides a*</u>, and write <u>$b|a$</u>, if there is an integer n such that <u>$a = bn$</u>, then b is <u>*divisor*</u> of a, or a is <u>*multiple*</u> of b.

  We also say for b nonzero: b divides a or b is a factor of a

- Theorem 4.3:
  a) $1 \mid a$ and $a \mid 0$ $(a \neq 0)$
  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 $x \in \mathbf{Z}$
  e) If $x = y + z$, and a divides two of the three integers x, y, and z, then a divides the remaining integer.
  f) $[(a \mid b) \wedge (a \mid c)] \Rightarrow a \mid (bx + cy)$, ($bx + cy$ is called linear combination of b, c)
  g) For $1 \leq i \leq n, c_i \in \mathbf{Z}$. If a divides each c_i, then $a \mid (c_1 x_1 + c_2 x_2 + \cdots + c_n x_n)$

- Proof f) If $a \mid b$ and $a \mid c \Rightarrow b = am$ and $c = an$

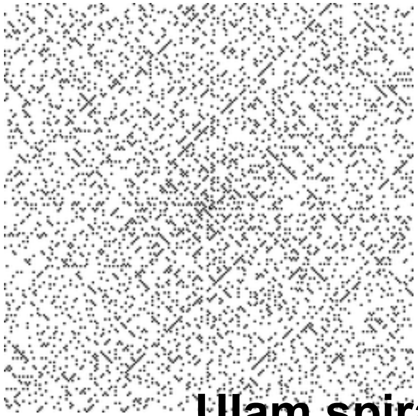
  $\therefore bx + cy = (am)x + (an)y = a(mx + ny)$

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

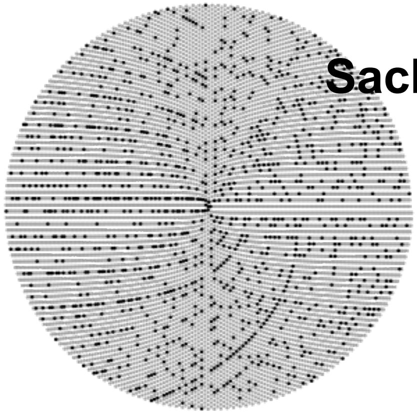
The Division Algorithm: Prime Numbers

- 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.



Ulam spiral, 1963



Sacks spiral, 1994

Primer Distribution, 2013

https://www.simonsfoundation.org/features/science-news/unheralded-mathematician-bridges-the-prime-gap/

The Division Algorithm: Prime Numbers

- 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.
    - By Well-Ordering Principle, S has a least element m.
    - If m is composite, then $m=m_1m_2$, $1<m_1<m$, $1<m_2<m$.
    - Since $m_1 \notin S$, m_1 is prime or divisible by a prime, so exists a prime p, $p|m_1$.
    - Since $p|m_1$ and $m=m_1m_2$, so $p|m$. (contradiction, Theorem 4.3 (d))

The Division Algorithm: Prime Numbers

- Theorem 4.4: There are infinitely many primes. (**Euclid**, Book IX)
  - Proof
    - If not
    - Let $p_1, p_2, \ldots, p_k$ be the finite list of all primes.
    - Let $B = p_1 p_2 \ldots p_k + 1$.
    - Since $B > p_i$, $1 \le i \le k$, B is not a prime.
    - So 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))

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

The Division Algorithm: Prime Numbers

- 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 $a = qb + r, 0 \le r < b$.

*We call r the **remainder** when a is divided by b, and q the **quotient** when a is divided by b.*

- Proof

(1) q, r exist

(a) $b \mid a$, i.e., $r = 0$

(b) $b \nmid a$, r > 0

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

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

(ii) If $a \le 0$ and let $t = a - 1$, then $a - tb = a - (a-1)b = a(1-b) + b$

$\because 1 - b \le 0$ and $a \le 0 \therefore a - tb > 0, S \neq \phi$

(c) $b \nmid a$, r < b

$\because S \neq \phi \therefore S$ has a least element $r, 0 < r = a - qb$ (Well – Ordering Principle)

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

(ii) If $r > b$, then $r = b + c = a - qb \Rightarrow c = a - (q+1)b \in S$,

contradicting r is the least element of S.

$\therefore r < b$

(2) q, r are unique

If there are other $q's$ and $r's$, let $a = q_1 b + r_1 = q_2 b + r_2$

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

$\therefore q_1 = q_2$ and $r_1 = r_2$

The Division Algorithm: Prime Numbers

- **Ex 4.25**
  - If the dividend a =170 and the divisor b = 11, then the quotient q = 15, and the remainder r = 5. (170=15*11+5)
  - If the dividend a = 98 and the divisor b = 7, then the quotient q = 14, and the remainder r = 0. (98=14*7)
  - If the dividend a = -45 and the divisor b = 8, then the quotient q = -6, and the remainder r = 3. (-45=(-6)*8+3 or -45=(-5)*8-5?)
  - Let $a,b \in \mathbf{Z}^+$
    - If $a = qb$, then $-a = (-q)b$. So, the quotient is $\underline{-q}$, and the remainder is $\underline{0}$.
    - If $a = qb + r$, then $-a = (-q)b - r = (-q - 1)b + (b - r)$. So, the quotient is $\underline{-q - 1}$, and the remainder is $\underline{b - r}$.

```
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
         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
```

Figure 4.10

The Division Algorithm: Prime Numbers

- **Ex 4.27** : Write 6137 in the octal system (base 8)
  - Here we seek nonnegative integers $r_0, r_1, r_2, \ldots, r_k$, $0 < r_k < 8$, such that $6137 = (r_k \ldots r_2 r_1 r_0)_8$.
  - $$\begin{aligned} 6137 &= r_0 + r_1 \cdot 8 + r_2 \cdot 8^2 + \cdots + r_k \cdot 8^k \\ &= r_0 + 8(r_1 + r_2 \cdot 8 + \cdots + r_k \cdot 8^{k-1}) \\ &= 1 \cdot 8^4 + 3 \cdot 8^3 + 7 \cdot 8^2 + 7 \cdot 8 + 1 \\ &= (13771)_8 \end{aligned}$$

		remainders
8	6137	
8	767	1(r_0)
8	95	7(r_1)
8	11	7(r_2)
8	1	3(r_3)
	0	1(r_4)

How about base 2 and base 64?

The Division Algorithm: Prime Numbers

- **Ex 4.29** : Two's Complement Method: binary representation of negative integers
  - One's Complement: interchange 0's and 1's.
  - Add 1 to the prior result.
- Example: $6 \equiv 0110 \rightarrow 1001 + 0001 \rightarrow 1010 \equiv -6$
- Example: How do we perform the subtraction 33 – 15 in base 2 with patterns of 8-bits?
  - $$\begin{array}{rl} 00100001 & (33) \\ +11110001 & (-15) \\ \hline \cancel{1}\underline{00010010} & \end{array}$$

    $\boxed{00001111\ (+15)}$
- General formula: $x - y = x + [\underbrace{(2^n - 1) - y}_{\textit{One's complement of } y} + 1] - 2^n$

The Division Algorithm: Prime Numbers

- **Ex 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
    - Composite $n = n_1 n_2$
    - 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 $n_2 > \sqrt{n}$

      $n = n_1 n_2 > \sqrt{n}\,\sqrt{n} = n$ (contradiction)

    - So, assume $n_1 \leq \sqrt{n}$.

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

      (ii) If n_1 is not prime, there exists a prime $p < n_1$ where $p|n_1$. (Lemma 4.1)
      then $p < n_1 \leq \sqrt{n}$.
    - So $p|n$ and $p \leq \sqrt{n}$.

4.4 The Greatest Common Divisor: The Euclidean Algorithm

- Definition 4.3: For $a, b \in \mathbf{Z}$, a **positive** integer c is called a greatest common divisor of a, b if (最大公因數gcd(a,b))

  (a) $c|a$ and $c \mid b$ (c is a common divisor of a, b)

  (b) for any common divisor d of a and b, we have $d \mid c$

- 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 ?

The Greatest Common Divisor: The Euclidean Algorithm

- 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 and b.
  - Proof

Given $a,b\in\mathbf{Z}^+$, let $\underline{S=\{as+bt \mid s,t\in\mathbf{Z}, as+bt>0\}}$

S has a least element c (Well-Ordering Principle)

(i) Existence: We claim that c is a greast common divisor of a,b.

$\because c\in S, c=ax+by$, if $d|a$ and $d|b$, then $d|ax+by$ (Theorem 4.3(f))

$\therefore d\mid c$

If $c\nmid a, a=qc+r, 0<r<c$

then $r=a-qc=a-q(ax+by)=(1-qx)a+(-qy)b$

$\therefore r\in S$, contrdicting c is the least element of S

$\therefore c\mid a$, similarly, $c\mid b$

(ii) Uniqueness: If c_1, c_2 both are the greast common divisors

then $c_2\mid c_1$ and $c_1\mid c_2$

$\therefore c_1=c_2$ (Theorem 4.3(b))

The Greatest Common Divisor: The Euclidean Algorithm

- The greatest common divisor of a and b is denoted by $gcd(a, b)$.
  - gcd(a, b) = gcd(b, a)
  - Also, $a \in \mathbf{Z}$, if a $\neq$ 0, then gcd(a, 0) = $|a|$
- gcd(a, b) = the **smallest** positive integer of the **linear combination** of a and b
- a and b are called relatively prime when gcd(a, b)=1
  - i.e, $x, y \in \mathbf{Z}$ with $ax + by = 1$.
- gcd(a, b)=c → gcd(a/c, b/c)=1

- **Ex 4.33**
  - gcd(42, 70) = 14, 42x+70y=14
    - One solution x=2, y=-1
    - x=2-5k, y=-1+3k

The Greatest Common Divisor: The Euclidean Algorithm

- 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:

$$
\begin{array}{ll}
r_0 = q_1 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_2 r_2 + r_3 & 0 < r_3 < r_2 \\
r_2 = q_3 r_3 + r_4 & 0 < r_4 < r_3 \\
\ldots & \\
r_{n-2} = q_{n-1} r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = q_n r_n &
\end{array}
$$

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

The Greatest Common Divisor: The Euclidean Algorithm

- Proof

$$r_0 = q_1 r_1 + r_2$$
$$r_1 = q_2 r_2 + r_3$$
$$r_2 = q_3 r_3 + r_4$$
$$\cdots$$
$$r_{n-2} = q_{n-1} r_{n-1} + r_n$$
$$r_{n-1} = q_n r_n$$

To verify that $r_n = \gcd(a, b)$

(i) Verify $c \mid r_n$, for any divisor c of a, b

If $c \mid r_0$ and $c \mid r_1 (r_0 = a, r_1 = b)$, and $r_0 = q_1 r_1 + r_2$

then $c \mid r_2 (\because r_0 = q_1 r_1 + r_2$, Theorem 4.3 (e))

Next $c \mid r_1$ and $c \mid r_2 \Rightarrow c \mid r_3$

Continuing down $\Rightarrow c \mid r_n$

(ii) Verify $r_n \mid a$ and $r_n \mid b$

From the last equation $r_n \mid r_{n-1}$

$\therefore r_n \mid r_{n-2} (\because r_{n-2} = q_{n-1} r_{n-1} + r_n$, Theorem 4.3 (e))

Continuing up, $[r_n \mid r_3 \wedge r_n \mid r_2] \Rightarrow r_n \mid r_1$

$[r_n \mid r_2 \wedge r_n \mid r_1] \Rightarrow r_n \mid r_0 (r_0 = a, r_1 = b)$

$\therefore r_n = \gcd(a, b)$

The Greatest Common Divisor: The Euclidean Algorithm

- **Ex 4.34** : find the gcd(250,111), and express the results as a linear combination of these integers.
  - **Solution**

	250	111	
*2	222		
	28		
		84	*3
		27	
*1	27		
	1		

$$250 = 2\cdot 111 + 28 \qquad 0 < 28 < 111$$

$$111 = 3\cdot 28 + 27 \qquad 0 < 27 < 28$$

$$28 = 1\cdot 27 + 1 \qquad 0 < 1 < 27$$

$$27 = 27\cdot 1 + 0$$

$$\therefore \gcd(250,111) = 1$$

$$1 = 28 - 1\cdot 27 = 28 - 1[111 - 3\cdot 28]$$

$$= (-1)111 + 4\cdot 28 = (-1)111 + 4[250 - 2\cdot 111]$$

$$= 250\cdot 4 + 111\cdot(-9)$$

In fact, it is not unique

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

$$\boxed{\gcd(-250, 111) = \gcd(250, -111) = \gcd(-250, -111) = \gcd(250, 111) = 1.}$$

The Greatest Common Divisor: The Euclidean Algorithm

- **Ex 4.35** : the integers $8n+3$ and $5n+2$ are relatively prime.
  - **Solution**

$$8n+3=1(5n+2)+(3n+1) \qquad 0<3n+1<5n+2$$

$$5n+2=1(3n+1)+(2n+1) \qquad 0<2n+1<3n+1$$

$$3n+1=1(2n+1)+n \qquad 0<n<2n+1$$

$$2n+1=2\cdot n+1 \qquad 0<1<n$$

$$n=n\cdot 1+0$$

$$\gcd(8n+3,5n+2)=1$$

How about gcd(n, n+1)?

How about gcd(a-b, a+b)?

$$\boxed{(8n+3)(-5)+(5n+2)(8)=-15+16=1}$$

The Greatest Common Divisor: The Euclidean Algorithm

- **An algorithm**: a list of precise instructions designed to solve a particular type of problem, not just one special case.
- **Ex 4.36** : Use Euclidean algorithm to develop a procedure (in pseudocode) that will find gcd(a, b) for all a, b $\in \mathbf{Z}^+$

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

The Greatest Common Divisor: The Euclidean Algorithm

- **Ex 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.
  - **Solution**

$$55 = 3 \cdot 17 + 4, \qquad 0 < 4 < 17$$

$$17 = 4 \cdot 4 + 1, \qquad 0 < 1 < 4$$

$$1 = 17 - 4 \cdot 4 = 17 - 4[55 - 3 \cdot 17]$$

$$= 13 \cdot 17 - 4 \cdot 55$$

The Greatest Common Divisor: The Euclidean Algorithm

- **Ex 4.38** : On the average, Brian debug a Java program in 6 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.
  - **Solution**

$$6x + 10y = 104 \Rightarrow 3x + 5y = 52$$

$$\gcd(3,5) = 1 \Rightarrow 1 = 3 \cdot 2 + 5 \cdot (-1)$$

$$\Rightarrow 52 = 3 \cdot 104 + 5 \cdot (-52) = 3(104 - 5k) + 5(-52 + 3k)$$

$$\because 0 \le x = 104 - 5k,\ 0 \le y = -52 + 3k$$

$$\therefore \frac{52}{3} \le k \le \frac{104}{5}$$

$$\Rightarrow \begin{cases} k = 18 : x = 14, y = 2 \\ k = 19 : x = 9,\ \ y = 5 \\ k = 20 : x = 4, y = 8 \end{cases}$$

The Greatest Common Divisor: The Euclidean Algorithm

- 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.
- 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 lcm(a, b).
- Theorem 4.9: Let $a,b,c \in \mathbf{Z}^+$,with c = lcm(a, b). If d is a common multiple of a and b, then $c|d$.
  - **Proof** If $c \nmid d, d = qc + r \quad 0 < r < c$

    $\because c = \text{lcm}(a,b) \therefore c = ma$

    also $d = na, na = qma + r \Rightarrow (n - qm)a = r$

    but $0 < r < c$, contradict the claim that c is the least common multiple

    $\therefore c \mid d.$

The Greatest Common Divisor: The Euclidean Algorithm

- Theorem 4.10: For $a,b \in \mathbf{Z}^+$, $ab = \text{lcm}(a, b) \cdot \text{gcd}(a, b)$
- **Ex 4.40** : By Theorem 4.10 we have
  - (a) For all $a,b \in \mathbf{Z}^+$, If a and b are relatively prime, then $\text{lcm}(a, b) = ab$.
  - (b) The computations in Examples 4.36 (a = 168, b = 456) establish the fact that gcd(168,458) = 24. As a result we find that lcm(a, b)?
  - Solution

$$\because \text{gcd}(168,456) = 24$$

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

4.5 The Fundamental Theorem of Arithmetic

- Lemma 4.2: If $a, b \in \mathbf{Z}^+$, and p is prime, then

$$p \mid ab \Rightarrow p \mid a \vee p \mid b.$$

  - Proof

$$\text{(i) } p \mid a$$

$$\text{(ii) } p \nmid a$$

$$\because p \text{ is prime } \therefore \gcd(p, a) = 1$$

$$\therefore px + ay = 1, (bx)p + (y)ab = b$$

$$\because p \mid p \text{ and } p \mid ab \qquad [(a \mid b) \wedge (a \mid c)] \Rightarrow a \mid (bx + cy)$$

$$\therefore p \mid b \text{ (Theorem 4.3 (f))}$$

- Lemma 4.3: Let $a_i \in \mathbf{Z}^+$. If p is prime and $p \mid a_1 a_2 \cdots a_n \Rightarrow p \mid a_i$ for some $1 \le i \le n$.

The Fundamental Theorem of Arithmetic

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

$$\text{If not} \Rightarrow \sqrt{2} = \frac{a}{b}, \text{ where } a,b \in \mathbf{Z}^+, \text{ and } \gcd(a,b) = 1$$

$$\therefore 2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2 \Rightarrow 2 \mid a^2 \Rightarrow 2 \mid a \text{ (Lemma 4.2)}$$

$$\therefore a = 2c \Rightarrow 2b^2 = a^2 = 4c^2 \Rightarrow b^2 = 2c^2, 2 \mid b^2 \Rightarrow 2 \mid b \text{ (Lemma 4.2)}$$

$$\because 2 \mid a \wedge 2 \mid b \therefore \gcd(a,b) \geq 2 \text{ (Contradiction)}$$

$$\boxed{\sqrt{p} \text{ is irrational for every prime p}}$$

The Fundamental Theorem of Arithmetic

- Theorem 4.11: Every integer $n > 1$ can be written as a product of primes uniquely, up to the order of the primes. ($n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$)
  - **Proof**

    (i) existence

    If not, m is 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 product of primes

    ($\because 1 < m_1, m_2 < m$)

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

    (ii) uniqueness : use Mathematical Induction (alternative form, for $n = 2,3,4,\cdots,n\text{-}1$ are true)

    Suppose $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} = q_1^{t_1} q_2^{t_2} \cdots q_r^{t_r}$ where p_i, q_j are primes,

    and $p_1 < p_2 < \cdots < p_k, q_1 < q_2 < \cdots < q_r$

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

    $\because p_1$ and q_j are primes $\Rightarrow p_1 = q_j$, similarly, $q_1 = p_i$

    $\because$ *if* $i > 1$, we can't find j $\ni p_1 = q_j < p_i = q_1 \therefore p_1 = q_1$

    $\Rightarrow n_1 = \frac{n}{p_1} = p_1^{s_1 - 1} p_2^{s_2} \cdots p_k^{s_k} = q_1^{t_1 - 1} q_2^{t_2} \cdots q_r^{t_r}$

    $\boxed{\because n_1 < n}$ $\therefore$ By induction hypothesis, $k = r, p_i = q_i, s_1 = t_1, s_i = t_i$

If p is prime and $p \mid a_1 a_2 \cdots a_n$

$\Rightarrow p \mid a_i$.

The Fundamental Theorem of Arithmetic

- **Ex 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?
  - **Solution** (i) For $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$

    The number of positive divisors of n is $(s_1 + 1)(s_2 + 1)\cdots(s_k + 1)$

    $29{,}338{,}848{,}000 = 2^8 3^5 5^3 7^3 11$

    $\therefore \text{answer} = (8+1)(5+1)(3+1)(3+1)(1+1) = 1728$

    (ii) $360 = 2^3 3^2 5$

    $\therefore \text{answer} = (8-3+1)(5-2+1)(3-1+1)(3+1)(1+1) = 576$

    (iii) For $s_1 = 8$, we have 5 choices (0,2,4,6,8)

    For $s_2 = 5$, we have 3 choices (0,2,4)

    For $s_3, s_4 = 3$, we have 2 choices (0,2)

    For $s_5 = 1$, we have 1 choices (0)

    $\therefore \text{answer} = 5 \cdot 3 \cdot 2 \cdot 2 \cdot 1 = 60$

The Fundamental Theorem of Arithmetic

- **Ex 4.46** : Can we find three consecutive positive integers whose product is a perfect square, i.e., $m(m+1)(m+2) = n^2$, $m,n\in\mathbf{Z}^+$?
  - **Solution**

Suppose such m, n exist

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

(Exercise 21 of Section 4.4)

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

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

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

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

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

So, we conclude that there are no such three consecutive positive integers.