

# Recursive Definitions

**Example (Fibonacci Numbers): Define**

$$F_0 \stackrel{\text{def}}{=} 0$$

$$F_1 \stackrel{\text{def}}{=} 1 \quad \text{and}$$

$$F_{n+1} \stackrel{\text{def}}{=} F_{n-1} + F_n \quad \text{for } n = 1, 2, 3, \dots .$$

It is easy to see by Induction, alternate form, that  $F_n$  is well-defined for  $n = 0, 1, \dots$

This is a **Recursive Definition** of the **Fibonacci Numbers**  $F_0, F_1, F_2, \dots$

Here are the first few:

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89 ...

Here is a Lisp function to compute them:

```
(defun Fibonacci (n)
  (cond ((= n 0) 0) ; ==>
        ((= n 1) 1) ; ==>
        (t (+ (Fibonacci (- n 2))
              (Fibonacci (- n 1)))))) ; ==>
```

Here is a fact about them:

For  $n = 0, 1, \dots$

$$S_n : \sum_{k=0}^n F_k^2 = F_n \times F_{n+1} .$$

**Proof:** This is true by inspection for  $n = 0$ .

Next,

$$\begin{aligned} \sum_{k=0}^{n+1} F_k^2 &= \sum_{k=0}^n F_k^2 + F_{n+1}^2 \\ &= F_n \times F_{n+1} + F_{n+1}^2 \\ &= F_{n+1}(F_n + F_{n+1}) = F_{n+1} \times F_{n+2} . \end{aligned}$$

In other words,  $S_n \implies S_{n+1}$  for  $n = 0, 1, \dots$ .  
By Induction, all the  $S_n$  are true. QED  
The Fibonacci numbers have the following explicit representation: let  $\alpha$  and  $\beta$  be the positive and negative roots

$$\frac{1 \pm \sqrt{5}}{2} \quad \text{of} \quad x = 1 + \frac{1}{x},$$

respectively. [ $\alpha$  is the **Golden Mean.**] Then, for  $n = 0, 1, 2, \dots$

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}. \quad (*)$$

Indeed,

$$\begin{aligned} \alpha^n + \alpha^{n-1} &= \alpha^{n+1} \left( \frac{1}{\alpha} + \frac{1}{\alpha^2} \right) \\ &= \alpha^{n+1} \times \frac{1}{\alpha} \times \left( 1 + \frac{1}{\alpha} \right) \\ &= \alpha^{n+1}, \end{aligned}$$

and similarly

$$\beta^n + \beta^{n-1} = \beta^{n+1}.$$

The right hand side of (\*) therefore satisfies the recurrence relation defining the Fibonacci numbers. The equality (\*) is obvious for  $n = 0, 1$ .

**Another Application** Let  $\{P_i : i \in \mathbb{N}\}$  be a set of statements.

Let us define  $P_1 \vee P_2 \vee \dots \vee P_n$ :

a)  $P_1 \vee P_2$  by truth table; and

b)  $P_1 \vee P_2 \vee \dots \vee P_{n+1} \iff (P_1 \vee \dots \vee P_n) \vee P_{n+1}$   
for  $n = 2, 3, 4, \dots$ .

Let us prove by induction the following statement  $S_n$ ,  $n = 3, 4, \dots$ :

for all  $r$  with  $1 \leq r < n$

$$\begin{aligned} & (P_1 \vee \dots \vee P_r) \vee (P_{r+1} \vee \dots \vee P_n) \\ \iff & P_1 \vee \dots \vee P_r \vee P_{r+1} \vee \dots \vee P_n \end{aligned}$$

For  $n = 3$ , this follows

from the associativity of  $\vee$ :

$$P_1 \vee (P_2 \vee P_3) \iff (P_1 \vee P_2) \vee P_3 \iff P_1 \vee P_2 \vee P_3$$

The basic step is done.

To prove that  $S_n \implies S_{n+1}$  for  $n \geq 3$ , we assume that  $S_n$  is true and deduce that then  $S_{n+1}$  is true. In other words we want to show that then for  $1 \leq r < n + 1$

$$\begin{aligned} & (P_1 \vee \cdots \vee P_r) \vee (P_{r+1} \vee \cdots \vee P_{n+1}) \\ \iff & P_1 \vee \cdots \vee P_r \vee P_{r+1} \vee \cdots \vee P_{n+1} \end{aligned}$$

First the case that  $r = n$ . Then

$$\begin{aligned} & (P_1 \vee \cdots \vee P_r) \vee (P_{r+1} \vee \cdots \vee P_{n+1}) \\ \iff & (P_1 \vee \cdots \vee P_n) \vee P_{n+1} \\ \iff & P_1 \vee \cdots \vee P_{n+1} \end{aligned}$$

is true by the recurrent definition above.

**Now if  $1 \leq r < n$  then**

$$\begin{aligned} & (P_1 \vee \cdots \vee P_r) \vee (P_{r+1} \vee \cdots \vee P_{n+1}) \\ \iff & (P_1 \vee \cdots \vee P_r) \vee [(P_{r+1} \vee \cdots \vee P_n) \vee P_{n+1}] \\ \iff & [(P_1 \vee \cdots \vee P_r) \vee (P_{r+1} \vee \cdots \vee P_n)] \vee P_{n+1} \\ \iff & (P_1 \vee \cdots \vee P_r \vee P_{r+1} \vee \cdots \vee P_n) \vee P_{n+1} \\ \iff & P_1 \vee \cdots \vee P_r \vee P_{r+1} \vee \cdots \vee P_n \vee P_{n+1} \end{aligned}$$

$$a_1 + a_2 + \cdots + a_n \text{ and } a_1 \times a_2 \times \cdots \times a_n$$

are defined along these lines, and the generalized associativity and commutativity are shown this way as well.

# The Division Algorithm

Recall that the universe is  $\mathbb{Z}$ .

**Definition:** For  $a, b \in \mathbb{Z}$  we say  $a$  divides  $b$  and write  $a|b$  if there exists a  $q \in \mathbb{Z}$  such that

$$b = qa .$$

In this case we also say that  $b$  is a  $\langle n$  integer  $\rangle$  multiple of  $a$  or that  $a$  is a divisor of  $b$ .

**Some Facts:** For all  $a, b, c, x, y, z \in \mathbb{Z}$

$1|a$  and  $a|0$       and       $[a|b \wedge b|a] \implies a = \pm b ;$

$[a|b \wedge b|c] \implies a|c$       and       $a|b \implies a|bc ;$

if  $z = x + y$  and  $a$  divides any two of  $x, y, z$

then it divides the third;

$$[c|a \wedge c|b] \implies c | \underbrace{(ax + by)}_{\text{a linear combination}} .$$

If  $c_i : i = 1, \dots, n$  are integer multiples of  $a$  then so is any **linear combination**

$$x_1c_1 + \dots + x_nc_n .$$

Every integer  $c$  has the “obvious” divisors  $c, -c, 1, -1$

The integers fall into four classes:

- 1) the set  $\{0\}$  containing only 0;
- 2) the set  $\{1, -1\}$  of **units** – these are the two numbers that have multiplicative inverses;
- 3) the set of integers  $p$  whose only divisors

are the obvious ones:  $p, -p, 1, -1$  – these are the **prime numbers**;  
4) the rest – these are called the **composite numbers**.

**Lemma:** Every non-unit  $n$  has a **prime divisor**.

**Proof:** a)  $2|0$ . Next, it suffices to show this for positive integers  $n$ . Why?

are the obvious ones:  $p, -p, 1, -1$  – these are the **prime numbers**;

4) the rest – these are called the **composite numbers**.

**Lemma:** Every non-unit  $n$  has a **prime divisor**.

**Proof:** a)  $2|0$ . Next, it suffices to show this for positive integers  $n$ . Why?

BWoC assume the set  $B$  of positive composites without prime divisors is not empty. Then it has a least element  $l$ . Not being a prime,  $l$  has a divisor  $k \neq 1, -1, l, -l$ :  $l = qk$  for some  $q$ . We can choose  $1 < k < l$ .  $k$  has a prime divisor. Why?

are the obvious ones:  $p, -p, 1, -1$  – these are the **prime numbers**;

4) the rest – these are called the **composite numbers**.

**Lemma:** Every non-unit  $n$  has a **prime divisor**.

**Proof:** a)  $2|0$ . Next, it suffices to show this for positive integers  $n$ . Why?

BWoC assume the set  $B$  of positive composites without prime divisors is not empty.

Then it has a least element  $l$ . Not being a prime,  $l$  has a divisor  $k \neq 1, -1, l, -l$ :  $l = qk$  for some  $q$ . We can choose  $1 < k < l$ .  $k$  has a prime divisor. Why?

Then so does  $l$ : here is the contradiction. To what?

are the obvious ones:  $p, -p, 1, -1$  – these are the **prime numbers**;

4) the rest – these are called the **composite numbers**.

**Lemma:** Every non-unit  $n$  has a **prime divisor**.

**Proof:** a)  $2|0$ . Next, it suffices to show this for positive integers  $n$ . Why?

BWoC assume the set  $B$  of positive composites without prime divisors is not empty.

Then it has a least element  $l$ . Not being a prime,  $l$  has a divisor  $k \neq 1, -1, l, -l$ :  $l = qk$  for some  $q$ . We can choose  $1 < k < l$ .  $k$  has a prime divisor. Why?

Then so does  $l$ : here is the contradiction. To what?

**QED**

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

**Proof:** BWoC assume there are only finitely many of them, say

$$p_1, p_2, \dots, p_n .$$

The integer

$$N \stackrel{\text{def}}{=} p_1 \times p_2 \times \dots \times p_n + 1$$

has a prime divisor: one of the primes above divides it, say  $p_i$ . Then  $p_i | 1$ , impossible. **QED**

**Theorem (Division Algorithm):** If  $a, b \in \mathbb{Z}$  with  $a > 0$  then there exist unique integers  $q, r$  with

$$b = qa + r \quad \text{and} \quad 0 \leq r < a .$$

## Proof of the Existence: Consider

$$S \stackrel{\text{def}}{=} \{b - ka : k \in \mathbb{Z}\} .$$

This set contains a positive ( $\geq 0$ ) integer; namely if  $b \geq 0$ , then  $b - 0a \in S$ , and if  $b < 0$  then  $b - ba = b(1 - a) \in S$ . The set  $S_+ \stackrel{\text{def}}{=} \{s \in S : s \geq 0\}$  is not empty. It has a least element  $r$ .  $r$ , being a member of  $S$ , is of the form  $r = b - qa$  for some  $q$ . Clearly  $b = qa + r$  and  $r \geq 0$ . It is left to be shown that  $r < a$ . BWoC assume  $r \geq a$ . Then

$$0 \leq r' \stackrel{\text{def}}{=} r - a = b - (q+1)a$$

would be a member of  $S$  smaller than  $r$ .

## Proof of the Uniqueness: Suppose

$$b = qa + r = q'a + r' \quad \text{with } 0 \leq r, r' < a .$$

**WLoG**  $r \leq r'$ . We subtract and get

$$0 = (q' - q)a + (r' - r) \quad \text{with } 0 \leq (r' - r) < a .$$

**This is only possible if**  $q' - q = 0$  **and then**  
 $r' - r = 0$ . **QED**