Direct Proofs

Why does a computer scientist need to know how to do proofs??

- When we study algorithms we need to know two things:
  - Does it fulfill it’s requirements?
    - If it doesn’t it is worthless. Worse case scenario, people die.
  - How long does it take to run?
- CS practitioners need to reason all the time: about algorithms, code, distributed systems, security protocols, and so on.
  - To reason about complicated systems correctly and fluently, it is necessary to be familiar with fundamental proof techniques, because these techniques capture the most expressive and sound reasoning idioms, patterns, and laws.

Directions for Writing Proofs

1. Copy the statement of the theorem to be proved onto your paper.
2. Clearly mark the beginning of your proof with the word PROOF.

Directions for Writing Proofs

3. Make your proof self contained
   - Explain the meaning and type of each variable (normally at the beginning).
     - “Suppose m and n are even integers…”
4. Write your proof in complete, grammatically correct sentences.

   Then $m+n = 2r + 2s = 2(r+s)$

Directions for Writing Proofs

5. Keep your reader informed about the status of each statement in your proof.
   - Your reader should never be in doubt about whether something in your proof has been assumed, established, or is still to be deduced.
     - If it is assumed use words like “Suppose” or “Assume”
     - If it is still to be shown use “We must show that”

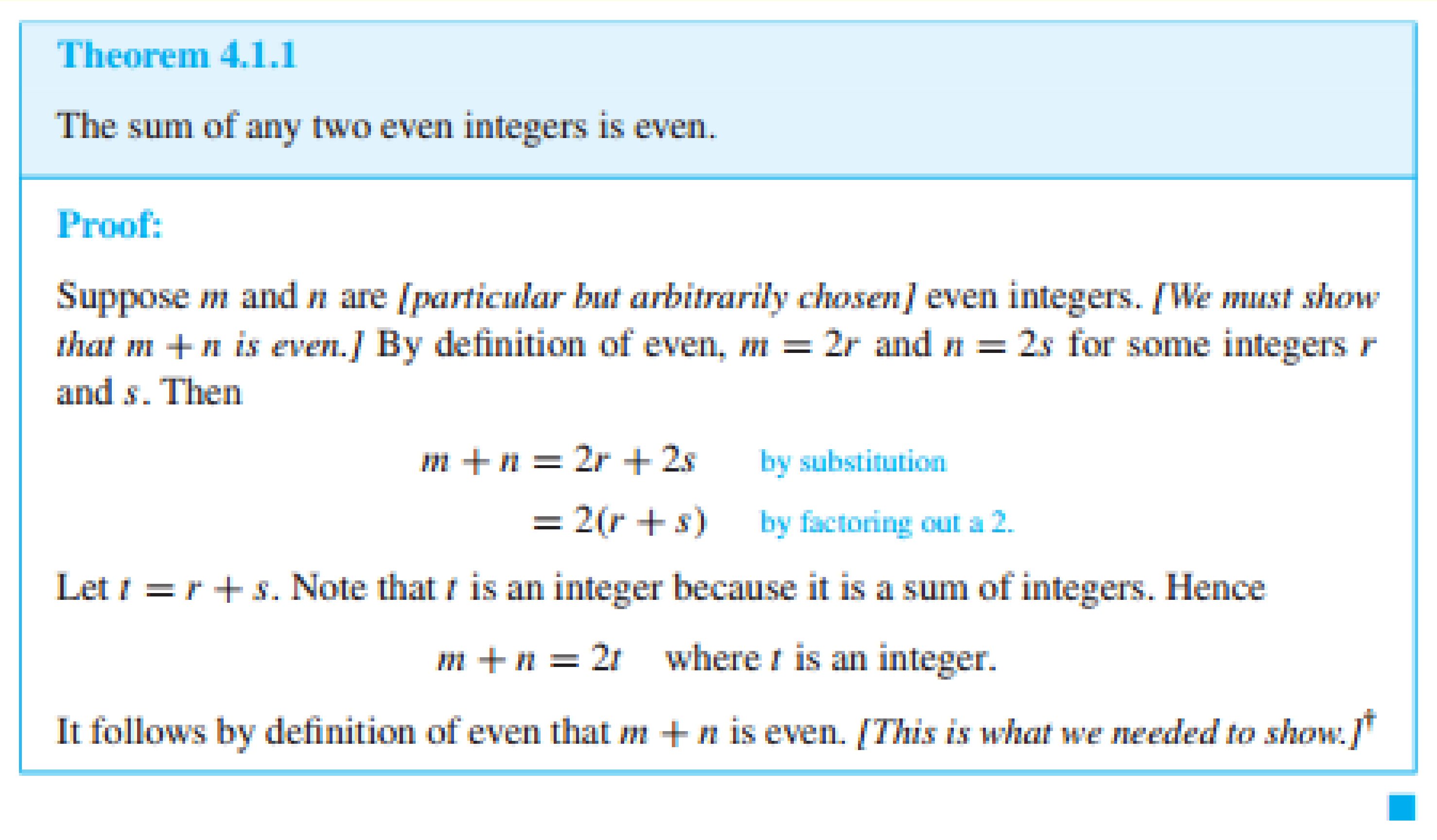
Directions for Writing Proofs

6. Give a reason for each assertion in your proof.
   - “By hypothesis”
   - “By definition of even, m=2r, where r is an integer”
7. Include the “little words” that make the logic clear
   - Thus, then, so, therefore, consequently, etc..

Directions for Writing Proofs

8. Clearly display equations and inequalities.
   - The convention is to display equations and inequalities on separate lines to increase readability.

Example



Theorem 4.1.1

The sum of any two even integers is even.

Proof:

Suppose m and n are *[particular but arbitrarily chosen]* even integers. *[We must show that $m + n$ is even.]* By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then

$$\begin{aligned} m + n &= 2r + 2s && \text{by substitution} \\ &= 2(r + s) && \text{by factoring out a 2.} \end{aligned}$$

Let $t = r + s$. Note that t is an integer because it is a sum of integers. Hence

$$m + n = 2t \quad \text{where } t \text{ is an integer.}$$

It follows by definition of even that $m + n$ is even. *[This is what we needed to show.]*[†] ■

Group Examples

Prove: For all integers n, if n is odd then n^2 is odd.

Group Examples

Prove: The negative of an even integer is even