

INTRODUCTION TO MATHEMATICAL REASONING

Worksheet 2

Definitions and Quantifiers

Exercise 1 (Solution) Sometimes in order to prove a mathematical statement to be true, it is easier to prove the contrapositive statement. This proof technique is called **proof by contradiction**. Fill in the blanks to complete the proof.

Theorem 1 There are infinitely many prime numbers.

Comment: This is another case where all the hypothesis are hidden: they consist of knowing the definition of prime numbers, and the usual axioms of arithmetics. So you should think of this theorem as the statement: “If the hidden hypothesis hold, then there are infinitely many prime numbers”. Therefore the contrapositive statement is: “If there are finitely many prime numbers, then something goes wrong in arithmetics”. What goes wrong is the following: if we assume there are finitely many prime numbers, and we take them all, then we can always produce one more prime number. Now let us write down this idea formally.

PROOF: Assume there are **finitely many** prime numbers, in particular we can assume there are n of them and we can write them $p_1, \dots, p_n$. Consider the number $q = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$, obtained by multiplying all the prime numbers together, and then adding 1. We claim that q is not divisible by **any** of the p_i 's. We prove this claim by contradiction.

Assume that q is **divisible** by one of the p_i 's, without loss of generality let us assume q is **divisible** by p_1 .

This means $q = p_1 \cdot k$, with k a natural number.

Then

$$q - p_1 \cdot p_2 \cdot \dots \cdot p_n = p_1(k - p_2 \cdot \dots \cdot p_n),$$

which shows that $q - p_1 \cdot p_2 \cdot \dots \cdot p_n$ is divisible by p_1 . But $q - p_1 \cdot p_2 \cdot \dots \cdot p_n = 1$ which is not divisible by any prime. Assuming that q is divisible by one of the p_i 's led to a contradiction, which allows us to conclude the claim: q is not divisible by **any** of the p_i 's. But then there are two possibilities: either q is a new prime number, or q has a prime factorization with primes that are different from the p_i 's. In either case, we are contradicting the statement that the list $p_1, \dots, p_n$ contains **finitely many** prime numbers. Assuming that there are finitely many primes led us to a contradiction, which shows that it must be the case that there are infinitely many prime numbers.

□