Mathematical Foundations of Computer Science
Lecture Outline
September 15, 2020

Example. Prove that the product of two odd numbers is an odd number.

Solution. Let x and y be particular but arbitrarily chosen odd numbers. Then, $x = 2k+1$ and $y = 2l + 1$, for some integers k and l. We have

$$x \cdot y = (2k + 1) \cdot (2l + 1) = 4kl + 2(k + l) + 1 = 2(2kl + k + l) + 1$$

Let $p = 2kl + k + l$. Since k and l are integers, p is an integer and $x \cdot y = 2p + 1$ is odd.

Example. Prove that $\sqrt{2}$ is irrational.

Solution. For the purpose of contradiction, assume that $\sqrt{2}$ is a rational number. Then there are integers a and b ($b \neq 0$) with no common factors such that

$$\sqrt{2} = \frac{a}{b}$$

Squaring both sides of the above equation gives

$$\begin{aligned} 2 &= \frac{a^2}{b^2} \\ a^2 &= 2b^2 \end{aligned} \tag{1}$$

From (1) we conclude that a^2 is even. This fact combined with the result of previous example implies that a is even. Then, for some integer k, let

$$a = 2k \tag{2}$$

Combining (1) and (2) we get

$$\begin{aligned} 4k^2 &= 2b^2 \\ 2k^2 &= b^2 \end{aligned}$$

The above equation implies that b^2 is even and hence b is even. Since we know a is even this means that a and b have 2 as a common factor which contradicts the assumption that a and b have no common factors.

We will now give a very elegant proof for the fact that "$\sqrt{2}$ is irrational" using the *unique factorization theorem* which is also called the *fundamental theorem of arithmetic*.

The unique factorization theorem states that every positive number can be uniquely represented as a product of primes. More formally, it can be stated as follows.

Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$$

and any other expression of n as a product of primes is identical to this except, perhaps, for the order in which the factors are written.

Example. Prove that $\sqrt{2}$ is irrational using the unique factorization theorem.

Solution. Assume for the purpose of contradiction that $\sqrt{2}$ is rational. Then there are integers a and b ($b \neq 0$) such that

$$\sqrt{2} = \frac{a}{b}$$

Squaring both sides of the above equation gives

$$\begin{aligned} 2 &= \frac{a^2}{b^2} \\ a^2 &= 2b^2 \end{aligned}$$

Let $S(m)$ be the sum of the number of times each prime factor occurs in the unique factorization of m. Note that $S(a^2)$ and $S(b^2)$ is even. Why? Because the number of times that each prime factor appears in the prime factorization of a^2 and b^2 is exactly twice the number of times that it appears in the prime factorization of a and b. Then, $S(2b^2) = 1 + S(b^2)$ must be odd. This is a contradiction as $S(a^2)$ is even and the prime factorization of a positive integer is unique.

Example. Prove or disprove that the sum of two irrational numbers is irrational.

Solution. The above statement is false. Consider the two irrational numbers, $\sqrt{2}$ and $-\sqrt{2}$. Their sum is $0 = 0/1$, a rational number.

Example. Show that there exist irrational numbers x and y such that x^y is rational.

Solution. We know that $\sqrt{2}$ is an irrational number. Consider $\sqrt{2}^{\sqrt{2}}$.

Case I: $\sqrt{2}^{\sqrt{2}}$ is rational.
In this case we are done by setting $x = y = \sqrt{2}$.

Case II: $\sqrt{2}^{\sqrt{2}}$ is irrational.
In this case, let $x = \sqrt{2}^{\sqrt{2}}$ and let $y = \sqrt{2}$. Then, $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2$, which is an integer and hence rational.

Example. Prove that for all positive integers n,

$$n \text{ is even} \leftrightarrow 7n + 4 \text{ is even}$$

Solution. Let n be a particular but arbitrarily chosen integer.
Proof for n is even $\rightarrow$ $7n + 4$ is even. Since n is even, $n = 2k$ for some integer k. Then,

$$7n + 4 = 7(2k) + 4 = 2(7k + 2)$$

Hence, $7n + 4$ is even.

Proof for $7n + 4$ is even $\rightarrow$ n is even. Since $7n + 4$ is even and n is a positive integer, let $7n + 4 = 2l$ for some integer $l \geq 6$. Then,

$$7n = 2l - 4 = 2(l - 2)$$

Clearly, $7n$ is even. Combining the fact that 7 is odd with the result of the Example 1, we conclude that n is even.

We can also prove the latter by proving its contrapositive, i.e., we can prove

$$\text{if } n \text{ is odd then } 7n + 4 \text{ is odd.}$$

Since n is a positive odd integer, we have $n = 2k + 1, \text{for some integer} k \geq 0$. Thus we have

$$\begin{aligned} 7n + 4 &= 7(2k + 1) + 4 \\ &= 14k + 10 + 1 \\ &= 2(7k + 5) + 1 \\ &= 2k' + 1, \text{where } k' = 7k + 5 \text{ is an integer.} \end{aligned}$$

Example. Prove that there are infinitely many prime numbers.

Solution. Assume, for the sake of contradiction, that there are only finitely many primes. Let p be the largest prime number. Then all the prime numbers can be listed as

$$2, 3, 5, 7, 11, 13, \ldots, p$$

Consider an integer n that is formed by multiplying all the prime numbers and then adding 1. That is,

$$n = (2 \times 3 \times 5 \times 7 \times \cdots p) + 1$$

Clearly, $n > p$. Since p is the largest prime number, n cannot be a prime number. In other words, n is composite. Let q be any prime number. Because of the way n is constructed, when n is divided by q the remainder is 1. That is, n is not a multiple of q. This contradicts

the Fundamental Theorem of Arithmetic.

Alternate Proof by Filip Saidak. Let n be an arbitrary positive integer greater than 1. Since n and $n+1$ are consecutive integers, they must be relatively prime. Hence, the number $N_2 = n(n+1)$ must have at least two different prime factors. Similarly, since the integers $n(n+1)$ and $n(n+1)+1$ are consecutive, and therefore relatively prime, the number

$$N_3 = n(n+1)[n(n+1)+1]$$

must have at least three different prime factors. This process can be continued indefinitely, so the number of primes must be infinite.

Mathematical Induction

Example. Prove that for all integers $n \geq 1$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Solution. We will prove the claim using induction on n.
Induction hypothesis: Assume that the claim is true when $n = k$, for some $k \geq 1$. In other words assume that

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

Base Case: $n = 1$. The claim is true for $n = 1$ as both sides of the equation equal to 1.
Induction step: To prove that the claim is true when $n = k+1$. That is, we want to show that

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

We can do this as follows.

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \\
&= \frac{k(k+1)}{2} + k + 1 \qquad \text{(using induction hypothesis)} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$