Mathematical Foundations of Computer Science
Lecture Outline
January 20, 2023

Example. Let x be an integer. If $x > 1$, then $x^3 + 1$ is composite.

Solution. Let x be an arbitrary but specific integer such that $x > 1$. We can rewrite $x^3 + 1$ as $(x+1)(x^2 - x + 1)$. Note that since x is an integer both $(x + 1)$ and $(x^2 - x + 1)$ are integers. Hence $(x + 1)|x^3 + 1$ and $(x^2 - x + 1)|x^3 + 1$. We now need to show that $x + 1 > 1$ and $x^2 - x + 1 > 1$. Since $x > 1$, clearly, $x + 1 > 1$. $x^2 - x + 1 > 1$ by the following reasoning.

$$\begin{aligned} x &> 1 && \\ x^2 &> x && \text{(Multiplying both sides by } x.) \\ x^2 - x &> 0 && \text{(Subtracting both sides by } x.) \\ x^2 - x + 1 &> 1 && \text{(Adding 1 to both sides.)} \end{aligned}$$

We can also argue that $x^2 - x + 1 > 1$ by showing that $x + 1 < x^3 + 1$. Since $x > 1$ we have $x^2 > x$ and hence $x^2 > 1$. Multiplying both sides by x again we get $x^3 > x$. This means that $x + 1 < x^3 + 1$ and since $(x + 1)|x^3 + 1$, we conclude that $x^3 + 1$ is composite.

Note: One student asked the question that why can't we write $x^3 + 1$ as $x^3(1 + \frac{1}{x^3})$. The reason is that for an integer $x > 1$, $(1 + \frac{1}{x^3})$ is not an integer and the proof breaks down.

Example. Prove that, for all real numbers x and all integers m,

$$\lfloor x + m \rfloor = \lfloor x \rfloor + m$$

Solution. Let $x = y + \epsilon$, where y is the largest integer with value at most x and $0 \leq \epsilon < 1$. Then,

$$\begin{aligned} x + m &= y + \epsilon + m \\ \lfloor x + m \rfloor &= \lfloor y + m + \epsilon \rfloor \\ &= y + m \\ &= \lfloor x \rfloor + m \end{aligned}$$

Example. Prove that if x and y are integers where $x + y$ is even, then x and y are both odd or both even.

Solution. To prove the above claim we will prove its contrapositive which is "if exactly one of x or y is even then $x + y$ is odd". Without loss of generality, for some integers k and l, let $x = 2k$ be even and $y = 2l + 1$ be odd. Then,

$$\begin{aligned} x + y &= 2k + 2l + 1 \\ &= 2(k + l) + 1 \end{aligned}$$

Since k and l are integers so is $k + l$ and $2(k + l)$ is even and hence $x + y$ is odd.

Example. Show that at least three of any 25 days chosen must fall in the same month of the year.

Solution. Assume for contradiction that the proposition "at least three of any 25 days chosen must fall in the same month of the year" is not true. This means that each month can have at most two of the 25 days chosen. Since there are 12 months, there can be at most 24 days that must have been chosen. This contradicts the premise that we chosen 25 days. In other words, by assuming that the proposition in the question is false, we have proved that (25 days are chosen) and (at most 24 days are chosen), which is clearly a contradiction.

Example. If $3n + 2$ is odd then n is odd.

Solution. We will show the above claim is true by giving a proof by contradiction. Thus assume that $3n + 2$ is odd and n is even. Since n is even, there exists an integer k such that $n = 2k$. Thus $3n + 2$ can be written as

$$3(2k) + 2 = 2(3k + 1)$$

Since k is an integer, clearly $3k+1$ is an integer. Thus $3n+2$ is even. Note that our premise is that $3n + 2$ is odd and we have shown that $3n + 2$ is even. This is a contradiction. This proves the claim.

Example. Prove that for all real numbers a and b, if the product ab is an irrational number, then either a or b, or both must be irrational.

Solution. We will prove the above claim by proving the contrapositive. That is, we will show that if both a and b are rational numbers then their product ab is a rational number. Let $a = p/q$ and $b = r/s$, where p, q, r, and s are integers and $q \neq 0$ and $s \neq 0$. The product ab can be expressed as follows.

$$ab = \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$$

Note that the numerator pr is an integer and so is the denominator qs. Also, since $q \neq 0$ and $s \neq 0$, the denominator $qs \neq 0$. Thus ab is a rational number.

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.