Mathematical Foundations of Computer Science
Lecture Outline
September 10, 2024

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

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

Note that since $1 < \sqrt{2} < 2$, we can assume that $a > 1$ and $b > 1$. 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.

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

Example. Prove that the sum of the first n positive odd numbers is n^2.

Solution. We want to prove that $\forall$ positive integers $n, P(n)$ where $P(n)$ is the following property.

$$\sum_{i=0}^{n-1} 2i+1 = n^2$$

Base Case: We want to show that $P(1)$ is true. This is clearly true as

$$\sum_{i=0}^{0} 2i+1 = 1 = 1^2$$

Induction Hypothesis: Assume $P(k)$ is true for some $k \geq 1$.
Induction Step: We want to show that $P(k+1)$ is true, i.e., we want to show that

$$\sum_{i=0}^{k} 2i+1 = (k+1)^2$$

We can do this as follows.

$$\begin{aligned} \sum_{i=0}^{k} 2i+1 &= \sum_{i=0}^{k-1} 2i+1+2k+1 \\ &= k^2+2k+1 \qquad \text{(using induction hypothesis)} \\ &= (k+1)^2 \end{aligned}$$

Example. Show that for all integers $n \geq 0$, if $r \neq 1$,

$$\sum_{i=0}^{n} ar^i = \frac{a(r^{n+1}-1)}{r-1}$$

Solution. Let r be any real number that is not equal to 1. We want to prove that $\forall$ integers $n, P(n)$, where $P(n)$ is given by

$$\sum_{i=0}^{n} ar^i = \frac{a(r^{n+1}-1)}{r-1}$$

Base Case: We want to show that $P(0)$ is true.

$$\sum_{i=0}^{0} ar^i = a = \frac{a(r-1)}{r-1}$$

Induction Hypothesis: Assume that $P(k)$ is true for some integer $k \geq 0$.
Induction Step: We want to show that $P(k+1)$ is true, i.e., we want to prove that

$$\sum_{i=0}^{k+1} ar^i = \frac{a(r^{k+2}-1)}{r-1}$$

We can do this as follows.

$$\begin{aligned}
\text{L.H.S.} &= \sum_{i=0}^{k+1} ar^i \\
&= \sum_{i=0}^{k} ar^i + ar^{k+1} \\
&= \frac{ar^{k+1} - a}{r-1} + ar^{k+1} \\
&= \frac{a(r^{k+1}-1)}{r-1} + \frac{ar^{k+1}(r-1)}{r-1} \\
&= \frac{a}{r-1}\left(r^{k+1}(1+r-1) - 1\right) \\
&= \frac{a}{r-1}\left(r^{k+2} - 1\right) \\
&= \frac{a(r^{k+2}-1)}{r-1}
\end{aligned}$$

Example. Prove that $\forall$ non-negative integers n,

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

Solution. By setting $a = 1$, $r = 2$ in the result of the previous problem, the claim follows.

Example. Prove that $\forall$ non-negative integers n, $2^{2n} - 1$ is a multiple of 3.

Solution. We want to prove that $\forall$ non-negative integers n, $P(n)$, where $P(n)$ is

$$2^{2n} - 1 = 3k, \text{ for some non-negative integer } k$$

Base Step: $P(0)$ is true as shown below.

$$2^0 - 1 = 0 = 3 \cdot 0.$$

Induction Hypothesis: Assume that $P(x)$ is true for some integer $x \geq 0$, i.e., $2^{2x} - 1 = 3 \cdot k'$, for some $k' \geq 0$.
Induction Step: We want to prove that $P(x+1)$ is true, i.e., we want to show that

$$2^{2(x+1)} - 1 = 3l, \text{ for some non-negative integer } l.$$

We can show this as follows.

$$\begin{aligned}
\text{L.H.S.} &= 2^{2(x+1)} - 1 \\
&= 2^{2x+2} - 1 \\
&= 2^{2x} \cdot 2^2 - 1 \\
&= 2^{2x} \cdot 4 - 1 \\
&= 2^{2x} \cdot (3+1) - 1 \\
&= 3 \cdot 2^{2x} + 2^{2x} - 1 \\
&= 3 \cdot 2^{2x} + 3 \cdot k' \qquad \text{(using induction hypothesis)} \\
&= 3(2^{2x} + k') \\
&= 3l, \qquad \text{where } l = 2^{2x} + k'
\end{aligned}$$

Since x and k' are integers l is also an integer. Hence, $P(x+1)$ is true.

Example. Prove that $\forall n \in \mathbb{N}, n > 1 \to n! < n^n$.

Solution. Below is a simple direct proof for this inequality.

$$\begin{aligned}
n! &= 1 \times 2 \times 3 \times \cdots \times n \\
&< n \times n \times n \times \cdots \times n \\
&= n^n
\end{aligned}$$

We now give a proof using induction. Let $P(n)$ denote the following property.

$$n! < n^n$$

Induction Hypothesis: Assume that $P(k)$ is true for some integer $k > 1$.
Base Case: We want to prove $P(2)$. $P(2)$ is the proposition that $2! < 2^2$, or $2 < 4$, which is true.
Induction Step: We want to prove $P(k+1)$, i.e., we want to prove that $(k+1)! < (k+1)^{k+1}$.

$$\begin{aligned}
\text{L.H.S.} &= (k+1)! \\
&= k! \times (k+1) \\
&< k^k \times (k+1) \qquad \text{(using induction hypothesis)} \\
&< (k+1)^k \times (k+1) \quad \text{(since } k > 1\text{)} \\
&= (k+1)^{k+1}
\end{aligned}$$