M 328K: Lecture 2

Katherine Ho

August 29, 2024

1 Proof by Contradiction

To prove a statement p, assume p is false and derive a contradiction.

Theorem 1.1. *$\sqrt{2}$ is irrational.*

Proof. Assume $\sqrt{2}$ is rational. So there exist integers a,b s.t.

$$\sqrt{2} = \frac{a}{b}, \text{ where a and b have no common factors.}$$

Thus $2b^2 = a^2$. ie. $2|a^2$. Hence also $2|a$. By definition, we can write $a = 2k$ for some $k \in \mathbb{Z}$. Then,

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

So $2|b^2$, hence $2|b$. Thus, 2 is a common factor of a and b, a contradiction.
Therefore, $\sqrt{2}$ is irrational. □

2 Proof by Induction

Use to prove an infinite number of statements. Ex: Prove that the sum of the first n odd integers is n^2.
Strategy:

- Prove base case(s) n=0,1
- Prove that if the statement is true for n, then it is true for n+1

Proof by Induction. Base case: For n=1, the sum of the first n positive odd integers is 1, which is n^2.
Induction step: Assume that the sum of the first n odd integers is n^2. Consider the sum of the first n+1 odd integers.

$$\sum_{k=1}^{n+1} 2k - 1 = 1 + 3 + 5 + \cdots + 2n - 1 + 2(n+1) - 1$$

By the induction hypothesis, we have

$$\begin{aligned} \sum_{k=1}^{n+1} 2k - 1 &= n^2 + 2(n+1) - 1 \\ &= n^2 + 2n + 2 - 1 \\ &= n^2 + 2n + 1 \\ &= (n+1)^2, \text{ as desired} \end{aligned}$$

□

Theorem 2.1. *For $n \geq 1$, $\frac{d}{dx}x^n = nx^{n-1}$.*

Proof by Induction. Base case: n=1. $\frac{d}{dx}x^1 = 1 = 1 \cdot x^0$.
Induction step: Assume $\frac{d}{dx}x^n = nx^{n-1}$ is true for some $n > 1$. Using the power rule, we have

$$\begin{aligned}\frac{d}{dx}x^{n+1} &= x(nx^{n-1}) + x^n \\ &= n \cdot x^{1+(n-1)} + x^n \\ &= x^n(n+1) \\ &= (n+1)x^n, \text{ as desired.}\end{aligned}$$

□

3 Well Ordering Principle (WOP)

Every nonempty subset of $\mathbb{N}$ has a smallest element.

Theorem 3.1 (Division Algorithm)**.** *For any $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique integers q,s s.t. $a = bq + r, 0 \leq r < |b|$.*

Proof. Consider the set

$$S = \{a - bx | x \in \mathbb{Z}, a - bx \geq 0\}$$

For simplicity, assume $b > 0$. Note that S is nonempty since for $x = -|a|$, we have

$$\begin{aligned}a - bx = a - b - (-|a|) &= a + b|a| \\ &\geq a + |a| \\ &\geq 0\end{aligned}$$

So, $a - bx \in S$.

By WOP, S has a smallest element r. Call the corresponding value of x by q.
So $r = a - bq \Leftrightarrow a = bq + r$.

Now, we want to show that $0 \leq r \leq |b|$ $(= b)$ since $b > 0$.
By way of contradiction, assume $r \geq b$. Consider

$$\begin{aligned}a - b(q+1) &= a - bq - b \\ &= r - b \\ &\geq 0\end{aligned}$$

Thus, $a - b(q+1)$ is an element of S that is smaller than r, a contradiction.

Suppose there exist $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such that

$$a = bq_1 + r_1 = bq_2 + r_2$$

where $0 \leq r_1, r_2 < b$ (still assuming $b > 0$). We want to show $q_1 = q_2, r_1 = r_2$. We have

$$\begin{aligned}bq_1 - bq_2 &= r_1 - r_2 \\ b(q_1 - q_2) &= r_1 - r_2 \\ b|q_1 - q_2| &= |r_1 - r_2| < b\end{aligned}$$

But $b|q_1 - q_2| < b$ implies (since $b > 0$) that

$$0 \leq |q_1 - q_2| < 1$$

So, $q_1 - q_2$ since $q_1, q_2 \in \mathbb{Z}$ Thus also $r_1 = r_2$. □

Note: The division algorithm lets us make statements like "Every integer can be expressed uniquely in the form $4k, 4k+1, 4k+2, or 4k+3$"

Theorem 3.2. *The square of every odd integer is of the form $8k + 1$.*

Proof. By the division algorithm, any odd integer n is of the form $n = 4k + 1$ or $4k + 3$.
In the 1st case,

$$\begin{aligned} n^2 &= (4k+1)^2 \\ &= 16k^2 + 8k + 1 \\ &= 8(2k^2 + 3k + 1) \end{aligned}$$

In the 2nd case,

$$\begin{aligned} n^2 &= (4k+3)^2 \\ &= 16k^2 + 24k + 9 \\ &= 8(2k^2 + 3k + 1) + 1 \end{aligned}$$

□

Definition 3.1. *For $a, b, c \in \mathbb{Z}$, if $c|a$ and $c|b$, we say that c is a common divisor and has the property that for any other common c of a and b that $d \geq c$, we call d the greatest common divisor of a and b, and write $d = \gcd(a, b)$.*