MATH 110 **Lecture notes – 12**

Non-constructive existence proofs

Previously, to prove a statement of the form $\exists x\ P(x)$ we were giving an example of x in the domain that makes $P(x)$ true. For example, to prove $\exists x \in \mathbb{Z}\ (x+5>3)$ we can give an example $x=0$ since for this value, $x+5=5>3$. This type of proof is called constructive.

Sometimes it may not be easy (or possible) to give a specific example of x in the domain that makes $P(x)$ true, yet, we may be able to prove that such x exists. This type of proof is called non-constructive.

Below are some examples of non-constructive proofs.

Intermediate Value Theorem (I.V.T.) If $f(x)$ is continuous on the interval $[a,b]$ and N is a value between $f(a)$ and $f(b)$, then there exists a number $c \in (a,b)$ such that $f(c)=N$.

Important special case: if either $f(a)<0<f(b)$ or $f(b)<0<f(a)$, then we can choose $N=0$, so the I.V.T. says that there exists a number $c \in (a,b)$ such that $f(c)=0$.

Example 1. Statement: $\exists x \in \mathbb{R}\ x^5+2x^3+x+7=0$.

Proof: Let $f(x)=x^5+2x^3+x-7$. Since $f(x)$ is a polynomial, it is continuous everywhere (meaning it is continuous on any interval). Since $f(0)=-7<0$ and $f(2)=43>0$, by the I.V.T., there is a number $c \in (0,2)$ such that $f(c)=0$.

There are other theorems in Calculus that allow us to give non-constructive proofs, such as Rolle's Theorem, Mean Value Theorem, and Monotone Convergence Theorem stated below, and many others.

Rolle's Theorem. If $f(x)$ is continuous on an interval $[a,b]$, differentiable on (a,b), and satisfies $f(a)=f(b)$, then there exists a number $c \in (a,b)$ such that $f'(c)=0$.

Mean Value Theorem. If $f(x)$ is continuous on an interval $[a,b]$ and differentiable on (a,b), then there exists a number $c \in (a,b)$ such that $f'(c)=\dfrac{f(b)-f(a)}{b-a}$.

Monotone Convergence Theorem. If a sequence $\{a_n\}$ is increasing (meaning $a_k \le a_m$ for all $k<m$) and bounded above (meaning there exists a number N such that $a_n \le N$ for all n), then it has a limit (that is, there exists $L \in \mathbb{R}$ such that $\lim\limits_{n\to\infty} a_n = L$). Similarly, if a sequence $\{a_n\}$ is decreasing and bounded below, then it has a limit.

Theorem. The number $\sqrt{2}$ is irrational.

Theorem. A decimal represents a rational number if and only if it is either finite (aka terminating) or periodic (aka repeating).

Example 2. Statement: there exists a digit n that appears infinitely many times in the decimal representation of $\sqrt{2}$.

Proof: Suppose every digit (from 0 to 9) appears finitely many times in the decimal representation of $\sqrt{2}$. Then this decimal representation contains finitely many digits, that is, it is a finite decimal. Then $\sqrt{2}$ must be rational, however, this is false.

Note: moreover, we can conclude that at least two digits are present in this decimal representation infinitely many times. However, we still do not have any idea about which digits these are.

Example 3. Statement: there exist irrational numbers a and b such that a^b is rational.

Proof: Consider $\sqrt{2}^{\sqrt{2}}$. This number is either rational or irrational. Let us consider both of these cases.

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Then let $a = b = \sqrt{2}$. Both a and b are irrational, but a^b is rational.

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Then let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. Both a and b are irrational, however, $a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$ is rational.

Note 1: since we know one of the above cases must take place, we know that such a and b exist. However, we do not have a specific example of a and b since we do not know which of the two cases actually takes place.

Note 2: it has been proved that the number $\sqrt{2}^{\sqrt{2}}$ is actually irrational, but this is a much harder proof. So sometimes a non-constructive proof is easier than a constructive one.

Note 3: the above statement can be proved differently (constructively) as well. For example, it can be shown that $b = \log_2 9$ is irrational, then for $a = \sqrt{2}$ we have $a^b = \sqrt{2}^{\log_2 9} = \sqrt{2}^{2\log_2 3} = 2^{\log_2 3} = 3$ is rational.

Definition. Prime numbers of the form n and $n+2$ are called twin primes. For example, 3 and 5 are twin primes; 5 and 7; 11 and 13; 17 and 19; etc.

It is a well-known conjecture (called the Twin Prime Conjecture) that there are infinitely many twin primes. However, this is still an open problem in mathematics (nobody knows if this statement is true).

Example 4. Statement: $\exists n \in \mathbb{N}(n = 1 \leftrightarrow$ (there exist infinitely many twin primes)).

Proof. Let us consider two cases.

Case 1: there are infinitely many twin primes. Then $n = 1$ is a number that makes the statement true.

Case 2: there doesn't exist infinitely many twin primes. Then $n = 2$ is a number that makes the statement true.

Note: The Twin Primes Conjecture in this example can be replaced with any other conjecture or any statement whose truth value we do not know.

Example 5. Statement: $\exists n \in \{1, 2\}$ (Player n in chess has a strategy that guarantees victory or a draw).

The game of chess does not have any element of luck and, theoretically, it is possible to compute all possible steps and all possible winning, losing, and draw positions. Clearly, one of the players has a strategy that would guarantee at least a draw. However, the game is sufficiently complicated and contains sufficiently many possible positions that such a computation is not practically possible. Thus nobody knows which player has such a strategy.

Note: the game of chess in this statement can be replaced with any other sufficiently complicated game.