Week 13

Juan Patricio Carrizales Torres

Section 2: Proof by contradiction

October 23, 2021

Curiously, the open sentence $P(x)$ can be proven to be logically equivalent to $\sim P(x) \Rightarrow \perp$ by using some fundamental logical equivalences in propositional logic, namely, $P(x) \equiv P(x) \vee \perp \equiv\sim (\sim P(x)) \vee \perp \equiv\sim P(x) \Rightarrow \perp$. Thus, if we prove, say by direct proof, $\sim P(x) \Rightarrow \perp$, then $P(x)$ is proven to be true. A common example of a contradiction is $C \wedge \sim C$ since a statement C can only have one binary truth value. Let's give an example to better illustrate this type of proof.

Let $R : \forall x \in S, P(x) \Rightarrow Q(x)$ be a quantified statement. Suppose we want to prove this by contradiciton and so we assume that $\sim R$ is true, namely, $\sim (\forall x \in S, P(x) \Rightarrow Q(x)) \equiv \exists x \in S, P(x) \wedge \sim Q(x)$. Then, we need to make some assumption or use some known fact C to continue with our proof. However, we end up with the conclusion that $\sim C$ is true. Therefore, it is shown, by direct proof, that if $\sim R$ is true, then the contradiction $C \wedge \sim C$ must be true; so R is proven to be true.

Problem 10. Prove that there is no largest negative rational number.

Proof. Assume, to the contrary, that there is some $r \in \mathbb{Q}^-$ such that r is the largest negative rational number, namely, for every $n \in \mathbb{Q}^-$, $n < r$. Since r is a negative rational number, it follows that $r/2 \in \mathbb{Q}^-$. Since $r < r/2 < 0$, we arrive at a contradiction. $\square$

Problem 11. Prove that there is no smallest positive irrational number.

Proof. Assume, to the contrary, that there is a smallest positive irrational number r. Since r is positive and irrational, it follows that $r/2$ is postitve and irrational. Because $0 < r/2 < r$, this leads to a contradiction. $\square$

Problem 12. Prove that 200 cannot be written as a sum of an odd integer and two even integers.

Proof. Suppose, to the contrary, that 200 can be written as a sum of an odd integer a and two even integers b and d. Then, $a = 2m + 1$, $b = 2n$ and $d = 2l$ for some $m, n, l \in \mathbb{Z}$. Therefore, $a + b + d = 2m + 1 + 2n + 2l = 2(m + n + l) + 1$. Since $m + n + l \in \mathbb{Z}$, it follows that $a + b + d = 200$ is odd, which contradicts the fact that 200 is even. $\square$

Problem 13. Use proof by contradiction to prove that if a and b are odd integers, then $4 \nmid (a^2 + b^2)$.

Proof. Assume, to the contrary, that a and b are odd integers such that $4 \mid (a^2 + b^2)$. Then, $a^2 + b^2 = 4c$ for some $c \in \mathbb{Z}$. Since a and b are odd, it follows that a^2 and b^2 are odd. Thus, $a^2 = 2m + 1$ and $b^2 = 2n + 1$ for some integers n and m. Therefore, $4c = 2(2c) = 2m + 1 + 2n + 1 = 2(m + n) + 1$. Since $2c$ and $m + n$ are integers, we arrive at the contradiction that an even number is equal to an odd number. $\square$

Problem 14. Prove that if $a \geq 2$ and b are integers, then $a \nmid b$ or $a \nmid (b + 1)$.

Proof. Let a and b be integers such that $a \geq 2$ and assume, to the contrary, that $a \mid b$ and $a \mid (b+1)$. Then, $b = ac$ and $b+1 = ad$ for some integers c and d. Therefore, $b = ad - 1 = ac$ and so $ad - ac = a(d - c) = 1$. Since $d - c \in \mathbb{Z}$, it follows that $a \mid 1$, which is a contradiction since $a \geq 2$. $\square$

Problem 15. Prove that 1000 cannot be written as the sum of three integers, an even number of which are even.

Proof. Assume, to the contrary, that 1000 can be written as the sum of three integers a, b and c, an even number of which are even. Then we consider two cases.
Case 1. None of a, b and c are even (zero of them are even). Then, $a = 2m + 1$, $b = 2n + 1$ and $c = 2l + 1$ where $m, n, l \in \mathbb{Z}$. Therefore, $a + b + c = 2m + 1 + 2n + 1 + 2l + 1 = 2(m + n + l) + 3 = 2(m + n + l + 1) + 1 = 1000$. Since $m + n + l + 1 \in \mathbb{Z}$, the integer $a + b + c = 1000$ is odd, which contradicts the fact that 1000 is even.
Case 2. 2 of the integers a, b and c are even. Without loss of generality, let $a = 2m$, $b = 2n$ and $c = 2l + 1$ for integers m, n and l. Therefore, $a + b + c = 2m + 2n + 2l + 1 = 2(m + n + l) + 1 = 1000$. Because $m + n + l \in \mathbb{Z}$, the integer $a + b + c = 1000$ is odd, which contradicts the fact that 1000 is even. $\square$

Problem 16. Prove that the product of an irrational number and a nonzero rational number is irrational.

Proof. Assume, to the contrary, that there is an irrational number r and a nonzero rational number s such that $r \cdot s$ is rational. Then, $s = a/b$ where $a, b \in \mathbb{Z}$ such that $a \neq 0$ and $b \neq 0$. Thus, $r \cdot s = r \cdot (a/b) = c/d$ where $c, d \in \mathbb{Z}$ such that $d \neq 0$ and $c \neq 0$ (none of the factors is zero(rational number)). Since $a \neq 0$, we can multiply both sides by b/a. Thus $r = (cb)/(ad)$. Since $c \in \mathbb{Z}$ and $b \in \mathbb{Z}$, it follows that $cb \in \mathbb{Z}$. Because $a, d \in \mathbb{Z}$ and they are nonzero, it follows that $ad \in \mathbb{Z}$ and $ad \neq 0$, and so $r = (cb)/(cd)$ is a rational number, which contradicts our assumption that r was irrational. $\square$

Problem 17. Prove that when an irrational number is divided by a (nonzero) rational number, the resulting number is irrational.

Proof. Assume, to the contrary, that there are an irrational number r and nonzero rational number s such that r/s is rational. Then, $s = a/b$ where $a, b \in \mathbb{Z}$ and $a, b \neq 0$. Therefore, $r/s = r(b/a) = c/d$ where $c, d \in \mathbb{Z}$ and $c, d \neq 0$. Thus, $r = (ca)/(bd)$. Since $ca, bd \in \mathbb{Z}$ and $bd \neq 0$, it follows that $r = (ca)/(bd)$ is a rational number, which is a contradiciton. $\square$

Problem 18. Let a be an irrational number and r a nonzero rational number. Prove that if s is a real number, then either $ar + s$ or $ar - s$ is irrational.

Proof. Assume, to the contrary, that there are $a, s, r \in \mathbb{R}$ such that a is irrational, r is a nonzero rational number and both $ar + s$ and $ar - s$ are rational. Then, by the result proven in *Problem 16*, the number ar is an irrational number q. Therefore, $q + s = m/n$ and $q - s = k/l$ where $m, n, k, l \in \mathbb{Z}$ and $n, l \neq 0$. Thus, $q = m/n - s = k/l + s$. Note that,

$$\begin{aligned} \frac{m}{n} - \frac{k}{l} &= 2s \\ \frac{ml - kn}{2ln} &= s \end{aligned}$$

Since $(ml - kn), 2ln \in \mathbb{Z}$ and $2ln \neq 0$, it follows that s must be a rational number. However, this contradicts the proven *Result 15*, which states that the sum of an irrational and rational number, both $q + s$ and $q + (-s)$, is irrational. □

Problem 19. Prove that $\sqrt{3}$ is irrational. [Hint: First prove for an integer a that $3 \mid a^2$ if and only if $3 \mid a$. Recall that every integer can be written as $3q$, $3q + 1$ or $3q + 2$ for some integer q.]

Lemma 1. Let $a \in \mathbb{Z}$, then $3 \mid a^2$ if and only if $3 \mid a$.

Proof. Assume that $3 \mid a$. Then $a = 3b$ for some $b \in \mathbb{Z}$. Therefore, $a^2 = 9b^2 = 3(3b^2)$. Since $3b^2 \in \mathbb{Z}$, it follows that $3 \mid a^2$.
For the converse, assume that $3 \nmid a$. Then, either $a = 3q + 1$ or $a = 3q + 2$ for some $q \in \mathbb{Z}$. We consider these two cases.
Case 1. $a = 3q + 1$. Then $a^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$. Since $3q^2 + 2q \in \mathbb{Z}$, $3 \nmid a^2$.
Case 2. $a = 3q + 2$. Then $a^2 = 9q^2 + 6q + 4 = 3(3q^2 + 2q + 1) + 1$. Since $3q^2 + 2q + 1 \in \mathbb{Z}$, it follows that $3 \nmid a^2$.
Therefore, $3 \nmid a^2$. □

Result $\sqrt{3}$ is irrational

Proof. Assume, to the contrary, that $\sqrt{3}$ is rational. Then $\sqrt{3} = a/b$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. We may further assume that a/b has been reduced to its lowest terms. Therefore, $3 = a^2/b^2$ and so $a^2 = 3b^2$. Since $b^2 \in \mathbb{Z}$, it follows that $3 \mid a^2$ and, by lemma, $3 \mid a$; so $a = 3c$ where $c \in \mathbb{Z}$. Thus,

$$\begin{aligned} a^2 = 9c^2 &= 3b^2 \\ 3c^2 &= b^2 \end{aligned}$$

Since $c^2 \in \mathbb{Z}$, it follows that $3 \mid b^2$ and so, by lemma, $3 \mid b$; so $b = 3d$ where $d \in \mathbb{Z}$. Both $a = 3c$ and $b = 3d$ which contradicts our assumption that they were reduced to their lowest terms. □

Problem 20. Prove that $\sqrt{2} + \sqrt{3}$ is an irrational number.

Proof. Assume, to the contrary, that $\sqrt{2}+\sqrt{3}$ is a rational number. Then, $\sqrt{2}+\sqrt{3}=b$ where $b\in\mathbb{Q}$. Thus, $\sqrt{2}=b-\sqrt{3}$ and so $2=(b-\sqrt{3})^2=b^2-2b\sqrt{3}+3$. Note that,

$$\begin{aligned} 2 &= b^2-2b\sqrt{3}+3 \\ 2b\sqrt{3} &= b^2+1 \\ \sqrt{3} &= \frac{b}{2}+\frac{1}{2b} \end{aligned}$$

Therefore, $\sqrt{3}=b/2+1/2b$ is a rational number (sum of two rational numbers). However, this contradicts the fact that $\sqrt{3}$ is irrational. $\square$

Problem 21. (a)Prove that $\sqrt{6}$ is an irrational number.

Proof. Note that $3\mid 6$ and $2\mid 6$. Thus, a similar proof to the ones used to prove that $\sqrt{3}$ and $\sqrt{2}$ are irraitonal can be used.

Assume, to the contrary, that $\sqrt{6}$ is a rational number. Then, $\sqrt{6}=a/b$ where $a,b\in\mathbb{Z}$ and $b\neq 0$. We further assume that a/b is reduced to the lowest terms. Thus, $6=a^2/b^2$ and so $6b^2=2(3b^2)=a^2$. Since $3b^2\in\mathbb{Z}$, it follows that $2\mid a^2$ and, by *Theorem 3.12* (For integer x, x^2 is even iff x is even), $2\mid a$. Therefore, $a=2c$ for some integer c. Note that $a^2=(2c)^2=2(2c^2)=2(3b^2)$ and so $2c^2=3b^2$. Because $c^2\in\mathbb{Z}$, $2\mid 3b^2$. Therefore, by Theorem either $2\mid 3$ or $2\mid b^2$. Since $2\nmid 3$, it follows that $2\mid b^2$ and, by *Theorem 3.12*, $2\mid b$. Thus, $2\mid a$ and $2\mid b$, and so they have a divisor in common, which contradicts the fact the a/b was reduced to the lowest terms. $\square$

(b) Prove that there are infinitely many positive integers n such that $\sqrt{n}$ is irrational.

Proof. Assume, to the contrary, that there is a finite number of positive integers n such that $\sqrt{n}$ is irrational. Then, there must be some $m\in\mathbb{Z}^+$ such that $\sqrt{m}$ is irrational and for any irrational number $\sqrt{n}<\sqrt{m}$, where $n\in\mathbb{Z}^+$. Let $c\in\mathbb{Z}^+$ such that $c\geq 2$. Then, $\sqrt{m}<c\sqrt{m}$. Since c is a nonzero rational number and $\sqrt{m}$ is irrational, it follows by the result proven in *Problem 16* that $c\sqrt{m}$ is irrational. Because $c\in\mathbb{Z}^+$, $c\sqrt{m}=\sqrt{c^2m}$. Thus, $c^2m\in\mathbb{Z}^+$, $\sqrt{c^2m}$ is irrational and $\sqrt{m}<\sqrt{c^2m}$, which contradicts our initial assumption. $\square$

Problem 23. Prove that there is no integer a such that $a\equiv 5 \pmod{14}$ and $a\equiv 3 \pmod{21}$.

Proof. Assume, to the contrary, that there is an integer a such that $a\equiv 5 \pmod{14}$ and $a\equiv 3 \pmod{21}$. Then, $14\mid(a-5)$ and $21\mid(a-3)$, and so $a=14m+5$ and $a=21n+3$ where $m,n\in\mathbb{Z}$. Thus, $14m+5=21n+3$ and so $2=21n-14m=7(3n-2m)$. Since $3n-2m\in\mathbb{Z}$, it follows that $7\mid 2$ which is a contradiction. $\square$

Problem 24. Prove that there exists no positive integer x such that $2x<x^2<3x$.

Proof. Assume, to the contrary, that there is some positive integer x such that $2x<x^2<3x$. Since $x\in\mathbb{Z}^+$, if follows that $2<x<3$ (divide the original inequality by x). The number x must be greater than 2 and lower than 3, namely, in between two consecutive integers and therefore can not be an integer. This contradicts our initial assumption about x. $\square$

Problem 25. Prove that there do not exist three distinct positive integers a, b and c such that each integer divides the difference of the other two.

Proof. Assume, to the contrary, that there are three distinct positive integers a, b and c such that each divides the difference of the other two. Then, $a \neq b \neq c$, and without loss of generality it can be said that $b > a > c$. Therefore, $b \mid (a-c)$ and so $a - c = bm$ where $m \in \mathbb{Z}^+$ since $a - c > 0$. However, note that $bm \geq b > b - c > a - c > 0$, which leads to a contradiciton. $\square$

Problem 26. Prove that the sum of the squares of two odd integers cannot be the square of an integer.

Lemma 1. Let k be a positive odd integer. Then $\sqrt{2k}$ is an irrational number.

Proof. Assume, to the contrary, that there is some positive odd integer k such that $\sqrt{2k}$ is a rational number $m = a/b$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. We may further assme that a/b is reduced to the lowest terms. Then, $\sqrt{2k} = a/b$ and so $2k = a^2/b^2$. Therefore, $2kb^2 = a^2$ and so $2 \mid a^2$ and, by *Theorem 3.12*, $2 \mid a$. Thus, $a = 2c$ for some integer c and so $2kb^2 = 2(2c^2) = (2c)^2$. Therefore, $kb^2 = 2c^2$ and so $2 \mid kb^2$. Thus, by theorem, either $2 \mid k$ or $2 \mid b^2$. Since k is odd, it follows that $2 \mid b^2$ and so $2 \mid b$. Therefore, both $2 \mid a$ and $2 \mid b$, which means that they have a factor in common and contradicts our assumption. $\square$

Proof. Assume, to the contrary, that there are two odd integers a and b such that $a^2 + b^2 = k^2$ where $k \in \mathbb{Z}$. Then, $a = 2m + 1$ and $b = 2n + 1$ where $n, m \in \mathbb{Z}$, and so

$$\begin{aligned} a^2 + b^2 &= (2m+1)^2 + (2n+1)^2 \\ &= 4m^2 + 4m + 1 + 4n^2 + 4n + 1 \\ &= 2(2m^2 + 2m + 2n^2 + 2n + 1) \\ &= 2(2(m^2 + m + n^2 + n) + 1) = k^2 \end{aligned}$$

Then by squaring both sides we get $\sqrt{(2(2(m^2 + m + n^2 + n) + 1))} = |k|$. Since $m^2 + m + n^2 + n \in \mathbb{Z}$, it follows that $2(m^2 + m + n^2 + n) + 1$ is odd. Let $2(m^2 + m + n^2 + n) + 1 = l$. Therefore, by *lemma*, $\sqrt{2l}$ is an irrational number, which leads to a contradiciton. $\square$

Problem 27. Prove that if x and y are positive real numbers, then $\sqrt{x+y} \neq \sqrt{x} + \sqrt{y}$.

Proof. Assume, to the contrary, that there exist two positive real numbers x and y such that $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$. Squaring both sides we get $x + y = (\sqrt{x} + \sqrt{y})^2 = x + 2\sqrt{xy} + y$. Thus, $0 = 2\sqrt{xy}$ and therefore $xy = 0$, which leads to a contradiciton. $\square$

Problem 28. Prove that there do not exist positive integers m and n such that $m^2 - n^2 = 1$.

Proof. Assume, to the contrary, that there exist two positive integers m and n such that $m^2 - n^2 = 1$. Then, $m^2 - n^2 = (m+n)(m-n) = 1$. Therefore, both $(m+n) = (m-n) = 1$ since $m + n$ and $m - n$ are integers. However, since $m, n \in \mathbb{Z}^+$, it follows that $m + n > 1$ and this leads to a contradiciton. $\square$