MATH 220.201 CLASS 8 QUESTIONS

Today we started on proof by contradiction, so there are not many exercises yet. See Chapter 5 in the text (especially Ch 5.2) for many more examples. I encourage you to read the 'Three Prisoners' story at the end of Ch 5.2. Here I'll include the proofs we did in class.

Proposition 0.1. *There is no smallest positive real number.*

Before we prove this statement, let's parse what it is saying, using quantifiers. It's a nonexistence statement, so it should start $\sim \exists x....$ The whole thing is

$$\sim \exists x \in \mathbb{R}_{>0}, (\forall y \in \mathbb{R}_{>0}, x < y)$$

Proof. Suppose the proposition is false. Then there is a smallest positive real number x. Consider the number $x/2$. It is positive (because x is positive), and $x/2 < x$ (because x is positive). Therefore $x/2$ is a smaller positive real number. This contradicts our assumption!

Therefore, the proposition is true. □

Note that

$$\sim \exists x \in \mathbb{R}_{>0}, (\forall y \in \mathbb{R}_{>0}, x < y) \equiv \forall x \in \mathbb{R}_{>0}, (\exists y \in \mathbb{R}_{>0}, x \not< y)$$

So one could prove the statement directly instead, by proving this equivalent quantified statement. The proof will look very similar to what we did above.

Proposition 0.2. *The sum of any rational number and any irrational number is an irrational number.*

One could instead phrase this as, 'For all real numbers x and y, if x is rational and y is irrational, then $x + y$ is irrational.' Thus, its negation is 'There exist real numbers x and y such that x is rational, y is irrational, and $x + y$ is rational.'

Proof by Contradiction. Suppose that the statement false. Then there exist a rational number x and an irrational number y such that $x + y$ is rational. Thus, there exist integers a, c and nonzero integer b, d such that $x = \frac{a}{b}$ and $x + y = \frac{c}{d}$. Then

$$y = (x + y) - x = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}$$

Since $bc - ad$ and bd are integers (with bd nonzero), y is rational. This contradicts the assumption that y is irrational!

Therefore, the original statement is true. □

Direct proof. For any statements (or open sentences) P, Q, R,

$$\begin{aligned}(P \wedge Q) \implies R &\equiv \sim (P \wedge Q) \vee R \\ &\equiv \sim P \vee \sim Q \vee R \\ &\equiv \sim (P \wedge \sim R) \vee \sim Q \\ &\equiv (P \wedge \sim R) \implies \sim Q\end{aligned}$$

Therefore, the open sentence

$$((x \text{ is rational}) \wedge (y \text{ is irrational})) \implies (x + y \text{ is irrational})$$

is equivalent to

$$((x \text{ is rational}) \wedge (x + y \text{ is rational})) \implies (y \text{ is rational})$$

So we will directly show that for all real numbers x and y, if x is rational and $x + y$ is rational, then y is rational. If x is rational and $x + y$ is rational, then there exist integers a, c and nonzero integers b, d such that $x = \frac{a}{b}$ and $x + y = \frac{c}{d}$. Then

$$y = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}$$

Since $bc - ad$ is an integer and bd is a nonzero integer, y is rational.

□

Proposition 0.3. *Let a, b be any integers with $a \geq 2$. Then a does not divide b or a does not divide $b + 1$.*[1]

Note that you could instead write this as 'For all $b \in \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ and all $a \in \{2, 3, 4, \ldots\}$, a does not divide b or a does not divide $b+1$.' This makes it a bit more clear what the negation is.

Proof. Suppose the result is false. Then there exist integers a and b with $a \geq 2$ such that a divides b and a divides $b + 1$. That means there are integers k, ℓ such that $b = ka$ and $b + 1 = \ell a$. Then

$$1 = (b + 1) - b = \ell a - ka = (\ell - k)a$$

Thus, $a|1$. But this is impossible because $a \geq 2$! Therefore, the result is true. □

Another way to finish the proof is to say that $\frac{1}{a} = \frac{b+1}{a} - \frac{b}{a} = \ell - k$ is an integer, but this is impossible because $a \geq 2$.

Theorem 0.4. *The real number $\sqrt{2}$ is not rational.*

To prove this theorem, we need the following lemma.

Lemma 0.5. *Let n be an integer. Then if n^2 is even, n is even.*

Proof. We prove the contrapositive, namely that if n is odd, n^2 is odd. If n is odd, then $n = 2k + 1$ for some integer k. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is odd, as desired. □

[1] Remember, that we say *a divides b* if there is an integer k such that $b = ka$.

Proof of 0.4. Suppose for a contradiction that $\sqrt{2}$ is rational. Then it can be written as $\sqrt{2} = \frac{a}{b}$ for some integers a and b. Let d be the greatest common factor[2] of a and b. Then a/d and b/d are integers with no common factor such that $\sqrt{2} = \frac{a/d}{b/d}$. Thus, we may have assumed without loss of generality that a and b have no common factors.[3]

$$\begin{aligned} \sqrt{2} = \frac{a}{b} &\implies 2 = \frac{a^2}{b^2} &&\implies 2b^2 = a^2 \\ &\implies a^2 \text{ is even} &&\implies a \text{ is even} \end{aligned}$$

So let $a = 2c$ for some integer c.

$$\begin{aligned} 2b^2 = a^2 &\implies 2b^2 = 4c^2 &&\implies b^2 = 2c^2 \\ &\implies b^2 \text{ is even} &&\implies b \text{ is even} \end{aligned}$$

But now we have a contradiction, because a and b are both divisible by 2! Therefore, our assumption that $\sqrt{2}$ was rational must be false. □

Embedded in this proof is the idea of *infinite descent*. That is, if $\sqrt{2} = \frac{a}{b}$, then we can divide out factors of 2 from a and b *ad infinitum*, which is impossible to do for natural numbers.

Theorem 0.6. *There are infinitely many prime numbers.*

Note that, because the natural numbers are totally ordered (for any two numbers, one is larger than the other), this theorem is equivalent to saying 'For any prime number p, there is a prime number q such that $q > p$.' To prove the statement, we need a lemma.

Lemma 0.7. *Every natural number greater than* 1 *has a prime factor.*

Proof. Suppose that the lemma is false. Then there is some natural number greater than 1 with no prime factors. Let n be the smallest one. If n were prime, then this would contradict the assumption, since n is a factor of itself. Then n can be written as $n = ab$ for some natural numbers a, b both greater than 1. Since n is the smallest natural number greater than 1 with no prime factors, a must have a prime factor p. Then $a = pk$ for some natural number k. Then $n = p(kb)$, and thus p is a prime factor of n. This is a contradiction! Therefore, the lemma holds true. □

Proof of 0.6. Suppose, for a contradiction, that there are finitely many prime numbers. Then there are n of them, for some natural number n. Call them $p_1, p_2, \ldots, p_n$. Now consider the number

$$N = p_1 p_2 \cdots p_n + 1$$

For each $i \in \{1, 2, \ldots, n\}$, p_i divides $N - 1$, and therefore by 0.3, p_i does not divide N. So N is a natural number which is not divisible by any prime number. Since $p_1 p_2 \cdots p_n$ is a natural number, $N = p_1 p_2 \cdots p_n + 1$ is greater than 1. But by the lemma, no such N can exist! Therefore, our assumption was false, and there are infinitely many prime numbers. □

[2]The fact that this is true is something I haven't yet proven, but I'll brush that under the rug for now.

[3]This is a common technique in nonexistence proofs. You assume for a contradiction that such an object exists, and then pick the 'smallest' one, for some notion of 'small'.

The algorithmic idea embedded in this proof allows you to generate new prime numbers from old ones.

$$\{2,3\} \mapsto 2 \cdot 3 + 1 = 7$$
$$\{2,3,7\} \mapsto 2 \cdot 3 \cdot 7 + 1 = 43$$
$$\{2,3,7,43\} \mapsto 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807 = 13 \cdot 139$$