12.5 = 13.1 (to review)

Proof by contradiction.

Idea: Prove $P \to (Q \wedge \neg Q)$.

Or $P \to C$, where C is a contradiction.

Can check: $(P \to C) \to \neg P$ is a tautology.

P	C	$\neg P$	$P \to C$	$(P \to C) \to \neg P$.
T	F	F	F	T
F	F	T	T	T

only F here.

Also known as "reductio ad absurdum".

"Reductio ad absurdum, which Euclid loved so much, is one of a math'n's finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a math'n offers the game."

Ex. For all nonequal positive real numbers x and y, we have $\frac{x}{y} + \frac{y}{x} > 2$

(12. Did outline of this proof — precise details carry on.)

Proof. Assume there are two nonequal positive real numbers x, y with $\frac{x}{y} + \frac{y}{x} \le 2$.

$$\text{Then, } \frac{x^2 + y^2}{xy} \le 2$$

12.6 = 13.2.

$$x^2 + y^2 \leq 2xy$$

$$x^2 - 2xy + y^2 \leq 0$$

$$(x-y)^2 \leq 0.$$

But this is only possible if $x - y = 0$, so $x = y$, contrary to hypothesis.

* Euclid's Elements, Prop 6. ("original Texts". Clark U.)

Prop 3.14] screen only.
3.17

with 3.17: ~~proof by contradiction~~
or: direct proof, ~~and use that an integer can't be both odd and even.~~

Rational and Irrational Numbers.

$\mathbb{N}$ = the natural numbers.

$\mathbb{Z}$ = the integers.

$\mathbb{Q}$ = the rational numbers.

$\mathbb{A}$ = algebraic numbers.

$\mathbb{R}$ = real numbers (limits).

$\mathbb{C}$ = complex numbers

$\mathbb{H}$ = quaternions $a + bi + cj + dk$

$i^2 = j^2 = k^2 = -1.$

$bc = -cb$, etc.

13.3.

Def. A real number x is rational if there exist integers m, n with $n \neq 0$ such that $x = \frac{m}{n}$. A real number that is not rational is called irrational.

Aside. The very formal def. Suppose you didn't have $\mathbb{R}$.

* Define $\mathbb{Q}$ as the set of all symbols $\frac{m}{n}$ with $n \neq 0$

$\frac{m}{n} = \frac{km}{kn}$ for all $k \in \mathbb{Z}$.

* Define an embedding of $\mathbb{Z}$ into $\mathbb{Q}$ by $m \mapsto \frac{m}{1}$.
* Define addition and multiplication. Prove that this respects your equivalence relation, the usual rules for arithmetic, it's closed.

Proposition. $\mathbb{Q}$ is closed under the usual arithmetic operations.

This means: If $x, y \in \mathbb{Q}$ then $x+y, x-y, xy \in \mathbb{Q}$.

If $y \neq 0$ then $\frac{x}{y} \in \mathbb{Q}$.

Can easily give direct proofs.

Prop. If x is rational and nonzero, and y is irrational, then xy is irrational.

13.4.

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

More specifically: if $r^2 = 2$, then r is irrational.

Number Theory Theorem. Any fraction $\frac{m}{n}$ can be written in lowest terms, such that no integers other than ± 1 divide both m and n.

Von Neumann – "In mathematics you don't understand things. You just get used to them."

Proof of Theorem. Assume to the contrary that $r^2 = 2$ for some rational number.

Then, we have $\left(\frac{a}{b}\right)^2 = 2$ for integers a and b, where a and b have no common factor.

and hence $a^2 = 2b^2$.

Thus, a^2 is even, and hence a is even. So we can write $a = 2c$ for some integer c. Thus

$$(2c)^2 = 2b^2$$

$$4c^2 = 2b^2$$

$$2c^2 = b^2.$$

Hence, b^2 is even, and so b is also even.

But then a and b have a common factor, a contradiction.

13.5.

Similar example. (Fermat)

Theorem. The equation $a^4 + b^4 = c^4$ has no nonzero integer solutions (a,b,c).

Proof. If there exists a solution, let (a,b,c) be the solution with minimal c. Then, ...

(find a smaller one).

NT Theorem. Every integer $n \geq 2$ is divisible by a prime.

Euclid's Theorem. There exist infinitely many primes.

Proof. Suppose to the contrary that there are only finitely many. Write $p_1 \cdots p_k$.

Consider

$$n = p_1 \cdots p_k + 1.$$

It cannot be prime, since it is larger than every prime. But then it must be divisible by a prime, which is one of the p_i.

However, since $p_i \mid p_1 \cdots p_k$, we see that dividing n by p_i leaves a remainder of 1, so it cannot be divisible by p_i.

This is a contradiction.

Not really any direct proof!

Evolution of proofs. Do Ex 19.