CLASS DISCUSSION: 24 OCTOBER 2019

PROOF BY CONTRADICTION

MODULAR ARITHMETIC

- **Attention!** Read and reread daily, **Writing Proofs**, pg 133 – 135.

REVIEW OF CHAPTER 5:

B. Prove the following statements using either direct or contrapositive proof. Sometimes one approach will be much easier than the other.

14. If $a, b \in \mathbb{Z}$ and a and b have the same parity, then $3a+7$ and $7b-4$ do not.

15. Suppose $x \in \mathbb{Z}$. If x^3-1 is even, then x is odd.

16. Suppose $x \in \mathbb{Z}$. If $x+y$ is even, then x and y have the same parity.

17. If n is odd, then $8 \mid (n^2-1)$.

18. For any $a, b \in \mathbb{Z}$, it follows that $(a+b)^3 \equiv a^3+b^3 \pmod 3$.

19. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod n$ and $a \equiv c \pmod n$, then $c \equiv b \pmod n$.

20. If $a \in \mathbb{Z}$ and $a \equiv 1 \pmod 5$, then $a^2 \equiv 1 \pmod 5$.

21. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod n$, then $a^3 \equiv b^3 \pmod n$

22. Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$. If a has remainder r when divided by n, then $a \equiv r \pmod n$.

23. Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod n$, then $ca \equiv cb \pmod n$.

24. If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv bd \pmod n$.

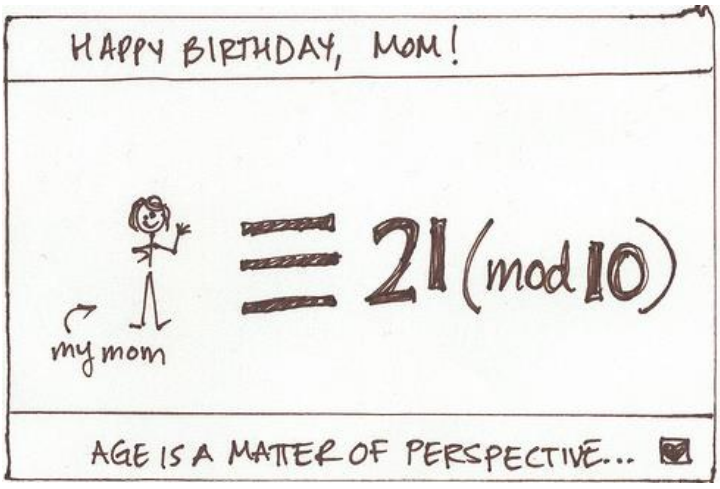
25. If $n \in \mathbb{N}$ and 2^n-1 is prime, then n is prime.

26. If $n = 2^k-1$ for $k \in \mathbb{N}$, then every entry in Row n of Pascal's Triangle is odd.

27. If $a \equiv 0 \pmod 4$ or $a \equiv 1 \pmod 4$, then $\binom{a}{2}$ is even.

28. If $n \in \mathbb{Z}$, then $4 \nmid (n^2-3)$.

MODULAR ARITHMETIC:



Define $a \equiv b \bmod m$ (for $m > 0$). Show that this is an equivalence relation on the set of integers, **Z**. In the following, assume that *a, b, c, d, m* are integers and that $m > 0$.

(A) Show that if $a \equiv b \bmod m$, then

1. $a + c \equiv b + c \bmod m$

2. $a - c \equiv b - c \bmod m$

3. $ac \equiv bc \bmod m$

(B) Show that if ac ≡ bc mod m (and *c* is not 0) then it need not follow that a ≡ b.

(C) Show that if d = gcd(c, m) and ac ≡ bc mod m, then a ≡ b mod m/d.

(D) Show that as a special case of the above we have:
If *c* and *m* are relatively prime and ac ≡ bc mod m, then a ≡ b mod *m*.

(E) Suppose that a ≡ b mod m and c ≡ d mod m. Prove that:

1) a + c ≡ b + d mod m

2) a – c ≡ b – d mod m

3) ac ≡ bd mod m

(F) Define addition and multiplication in Z_4 and in Z_5.

(G) Using modular arithmetic,

1) find the remainder when 2^{125} is divided by 7.

2) find the remainder when $(4^{19})(7^{99})$ is divided by 5.

PROOF BY CONTRADICTION

aka ***reductio ad impossibile***

Method

To prove a proposition P by contradiction:

1. Write, "We use proof by contradiction."
2. Write, "Suppose $\sim P$"
3. Deduce a logical contradiction C. (That is, find C for which $C \wedge \sim C$.)
4. Write, "This is a contradiction. Therefore, P must be true."

Example

Remember that a number is *rational* if it is equal to a ratio of integers. For example, $3.5 = 7/2$ and $0.1111\ldots = 1/9$ are rational numbers. On the other hand, we'll prove by contradiction that $\sqrt{2}$ is irrational.

Proposition: $\sqrt{2}$ *is irrational.*

Proof. We use proof by contradiction.

Suppose the claim is false; that is, $\sqrt{2}$ is rational.

Then we can write 2 as a fraction a/b in *lowest terms*.

Squaring both sides gives $2 = a^2/b^2$ and so $2b^2 = a^2$.
This implies that a is even; that is, a is a multiple of 2.
Therefore, a^2 must be a multiple of 4. Because of the equality $2b^2 = a^2$, we know $2b^2$ must also be a multiple of 4.
This implies that b^2 is even and so b must be even. But since a and b are both even, the fraction a/b is not in lowest terms.

This is a contradiction. Therefore, $\sqrt{2}$ must be irrational. □

Potential Pitfall

Often students use an indirect proof when a direct proof would be simpler. Such proofs aren't wrong; they just aren't excellent. Let's look at an example. A function f is *strictly increasing* if $f(x) > f(y)$ for all real x and y such that $x > y$.

Theorem. *If f and g are strictly increasing functions, then f + g is a strictly increasing function.*

Let's first look at a simple, direct proof.

Proof. Let x and y be arbitrary real numbers such that $x > y$. Then:

$f(x) > f(y)$ (since f is *strictly* increasing)

$g(x) > g(y)$ (since g is *strictly* increasing)

Adding these inequalities gives:

$$f(x) + g(x) > f(y) + g(y)$$

Thus, $f + g$ is strictly increasing as well. □

Now we *could* prove the same theorem by contradiction, but this makes the argument needlessly convoluted.

Proof. We use proof by contradiction. Suppose that $f + g$ is not strictly increasing. Then there must exist real numbers x and y such that $x > y$, but

$$f(x) + g(x) \leq f(y) + g(y)$$

This inequality can only hold if either $f(x) \leq f(y)$ or $g(x) \leq g(y)$. Either way, we have a contradiction because both f and g were defined to be strictly increasing. Therefore, $f + g$ must actually be strictly increasing. □

Exercises (As usual, assume unless otherwise stated, that our universe is Z.)

1. There is no smallest rational number greater than 0
2. If a is even then a^2 is even. Prove by contradiction.
3. If a ≥ 2, then $a \nmid b$ *or* $a \nmid (b+1)$
4. If n^2 is odd, then n is odd.
5. Prove that $\sqrt[3]{2}$ is irrational.
6. Prove that $a^2 - 4b - 3 \neq 0$ for any integers a, b.
7. Prove that there exist no integers, a and b, such that 21a + 30b = 1.
8. If A and B are arbitrary sets, then $A \cap (B - A) = \emptyset$.
9. Show that for any *n*, $4 \nmid (n^2 + 2)$.
10. Study the following proof (from our textbook). Is it logically correct?

Proposition If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.

Proof. Suppose this proposition is *false*.
This conditional statement being false means there exist numbers a and b for which $a, b \in \mathbb{Z}$ is true, but $a^2 - 4b \neq 2$ is false.
In other words, there exist integers $a, b \in \mathbb{Z}$ for which $\boxed{a^2 - 4b = 2.}$
From this equation we get $a^2 = 4b + 2 = 2(2b + 1)$, so a^2 is even.
Because a^2 is even, it follows that a is even, so $a = 2c$ for some integer c.
Now plug $a = 2c$ back into the boxed equation to get $(2c)^2 - 4b = 2$,
so $4c^2 - 4b = 2$. Dividing by 2, we get $2c^2 - 2b = 1$.
Therefore $1 = 2(c^2 - b)$, and because $c^2 - b \in \mathbb{Z}$, it follows that 1 is even.
We know 1 is **not** even, so something went wrong.
But all the logic after the first line of the proof is correct, so it must be that the first line was incorrect. In other words, we were wrong to assume the proposition was false. Thus the proposition is true. ■

Exercises:

11. Prove by contradiction that there exists no largest even integer.
12. Prove by contradiction that $\sqrt[3]{1332} > 11$.
13. There exist no integers a and b for which 21a+30b = 1.
14. Prove by contradiction that there exists no smallest positive real number.

15. Prove by contradiction that there exists no largest prime number. (Euclid's proof)

16. Prove by contradiction that $\sqrt{3}\ is\ irrational.$

17. Prove by contradiction that if x is irrational, then so is $x^{1/2}$.

18. Prove by contradiction that $2^{1/3}$ is irrational.

19. Suppose $n \in Z$. If n is odd, then n^2 is odd.

20. Suppose $n \in Z$. If n^2 is odd, then n is odd.

21. Prove by contradiction that if $0 \leq t \leq \pi/2$, then $\cos t + \sin t \geq 1$.

22. Let *n* be a positive integer. Prove that $\log_2 n$ is rational if and only if n is a power of 2.

23. Prove the arithmetic-geometric mean inequality by contradiction.

24. Employing the method of proof by contradiction show that for any non-degenerate triangle (that is, every side has positive length), the length of the hypotenuse is *less than* the sum of the lengths of the two remaining sides.

25. Let a and b be integers. If $a^2 + b^2 = c^2$, then a or b is even.

26. Prove that there are infinitely many prime numbers (Euclid).

G. H. Hardy described proof by contradiction as "one of a mathematician's finest weapons," saying "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 mathematician offers the game."

- G. H. Hardy, **A Mathematician's Apology**