CLASS DISCUSSION: 22 OCTOBER 2019

PROOF BY CONTRAPOSITIVE

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

Review of Direct Proofs:

Write *direct* proofs for each of the following, inserting parenthetical remarks to explain the rationale behind each step.

1. Prove that if *n* is the form 3K + 1, then n^2 is of the form 3L + 1.
2. Prove that if *n* is the form 5K + 3, then n^2 is of the form 5L + 4.
3. Let *n* be larger than 6. Prove that $n^2 - 25$ cannot be prime.
4. Let a, b, c, d $\in Z$. Prove that if a|b and c|d, then ac|bd.
5. Let *n* be an integer larger than 3. Then $n^3 - 8$ cannot be prime.
6. Prove that if *n* is odd, then n^3 is odd.
7. Let *a, b, c* be integers. Prove that if $a^2 \mid b$ and $b^3|c$, then $a^6|c$.
8. Let *x* and *y* be real numbers. Prove that if $x^2 + 5y = y^2 + 5x$ then either x = y or x + y = 5.
9. Let *m* and *n* be integers. Prove that if *m* and *n* are perfect squares, then mn is also a perfect square.

Prove each of the following by the *contrapositive method*.

1. If x and y are two integers for which x + y is even, then x and y have the same parity.
2. If x and y are two integers whose product is even, then at least one of the two must be even.
3. If x and y are two integers whose product is odd, then both must be odd.
4. If n is a positive integer of the form n = 3k + 2, then n is not a perfect square.
5. Let x$\in Z$. $If\ x^2 - 6x + 5\ is\ even, then\ x\ is\ odd.$
6. Let x, $y \in Z$. $If\ 7 \nmid xy, then\ 7 \nmid x\ and\ 7 \nmid y.$

Exercises for Chapter 5

A. Use the method of contrapositive proof to prove the following statements. (In each case you should also think about how a direct proof would work. You will find in most cases that contrapositive is easier.)

1. Suppose $n \in \mathbb{Z}$. If n^2 is even, then n is even.

2. Suppose $n \in \mathbb{Z}$. If n^2 is odd, then n is odd.

3. Suppose $a, b \in \mathbb{Z}$. If $a^2(b^2 - 2b)$ is odd, then a and b are odd.

4. Suppose $a, b, c \in \mathbb{Z}$. If a does not divide bc, then a does not divide b.

5. Suppose $x \in \mathbb{R}$. If $x^2 + 5x < 0$ then $x < 0$.

6. Suppose $x \in \mathbb{R}$. If $x^3 - x > 0$ then $x > -1$.

7. Suppose $a, b \in \mathbb{Z}$. If both ab and $a + b$ are even, then both a and b are even.

8. Suppose $x \in \mathbb{R}$. If $x^5 - 4x^4 + 3x^3 - x^2 + 3x - 4 \geq 0$, then $x \geq 0$.

9. Suppose $n \in \mathbb{Z}$. If $3 \nmid n^2$, then $3 \nmid n$.

10. Suppose $x, y, z \in \mathbb{Z}$ and $x \neq 0$. If $x \nmid yz$, then $x \nmid y$ and $x \nmid z$.

11. Suppose $x, y \in \mathbb{Z}$. If $x^2(y+3)$ is even, then x is even or y is odd.

12. Suppose $a \in \mathbb{Z}$. If a^2 is not divisible by 4, then a is odd.

13. Suppose $x \in \mathbb{R}$. If $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8$, then $x \geq 0$.

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 $4 \nmid (n^2 - 3)$.

Johann Carl Fredrich Gauss (1777–1855) introduced modular arithmetic.

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 $ac \equiv bc \bmod m$ (and *c* is not 0) then it need not follow that $a \equiv b$.

(C) Show that if $d = \gcd(c, m)$ and $ac \equiv bc \bmod m$, then $a \equiv b \bmod m/d$.

(D) Show that as a special case of the above we have:

If *c* and *m* are relatively prime and $ac \equiv bc \bmod m$, then $a \equiv b \bmod m$.

(E) Suppose that $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Prove that:

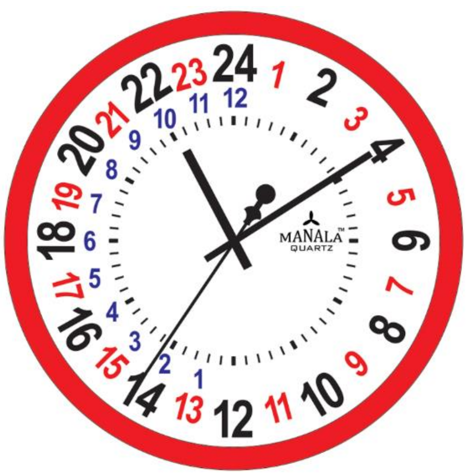
1. $a + c \equiv b + d \quad \bmod m$
2. $a - c \equiv b - d \quad \bmod m$
3. $ac \equiv bd \quad \bmod m$

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

(G) Using modular arithmetic,

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

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



The 24-hour time system has its origins in the Egyptian astronomical system of decans and has been used for centuries by scientists, astronomers, navigators, and horologists. In East Asia, time notation was 24-hour before westernization in modern times. Western-made clocks were changed into 12 dual-hours style when they were shipped to China in the Qing dynasty. There are many surviving examples of clocks built using the 24-hour system, including the famous Orloj in Prague, and the Shepherd Gate Clock at Greenwich.

(Wikipedia)