CLASS DISCUSSION: 27 OCTOBER 2019

PROOF BY CONTRAPOSITIVE

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

29. If integers a and b are not both zero, then $\gcd(a,b) = \gcd(a-b, b)$.

30. If $a \equiv b \pmod n$, then $\gcd(a,n) = \gcd(b,n)$.

31. Suppose the division algorithm applied to a and b yields $a = qb + r$. Then $\gcd(a,b) = \gcd(r,b)$.

Johann Carl Fredrich Gauss 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. $a + c \equiv b + d \mod m$

2. $a - c \equiv b - d \mod m$

3. $ac \equiv bd \mod m$

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

III 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.