1. Problems in Chapter 5

1.1. **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.

Proof. (contrapositive) Assume n is odd. $\square$

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

Proof. (contrapositive) Assume n is even. $\square$

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

Proof. (Contrapositive) Assume a is an even number. $\square$

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

Proof. (contrapositive) Assume there exists $q \in \mathbb{Z}$ so that $b = qa$. $\square$

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

Proof. (contrapositive) Assume $x \geq 0$. Then $x^2 + 5x = x(x + 5) \geq 0$. $\square$

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

Proof. (contrapositive) Assume $x \leq -1$. In that case, $x^3 - x = x(x + 1)(x - 1)$. $\square$

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

Proof. (contrapositive) Assume a is odd. $\square$

(8) **TODO** Suppose $x \in \mathbb{R}$. If $x^5 - 4x^4 + 3x^3 - x^2 + 3x - 4 \geq 0$, then $x \geq 0$.
- $x^5 - x^2 - 4(x^4 + 1) + 3(x^3 + x) = x^2(x^3 - 1) + 3x(x^2 + 1) - 4(x^4 + 1)$
- $x^5 + 3x^3 + 3x < 4x^4 + x^2 + 4$
- \(x(x^4 +3x^2 +3) <

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

Proof. (contrapositive) Assume n is a multiple of 3. $\square$

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

Proof. (contrapositive) Assume y is a multiple of x. $\square$

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

Proof. (contrapositive) Assume $x = 2a + 1$ and $y - 2b$ for some $a, b \in \mathbb{Z}$. $\square$

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

Proof. (contrapositive) Assume $a = 2x$ for some $x \in \mathbb{Z}$. $\square$

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

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

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

Case 1	Case 2
$a = 2x, b = 2y$ $3a+7 = 6x+7 = 2(3x+3)+1$ $7b-4 = 14x-4 = 2(7x-2)$	$a = 2x+1, b = 2y+1$ $3a+7 = 6x+10 = 2(3x+5)$ $7b-4 = 14y-11 = 2(7y-5)-1$

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

Proof. (contrapositive) Assume x is even. □

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

Proof. (contrapositive) Assume $x = 2a$ and $y = 2b + 1$ for integers a, b. □

(4) If n is odd, then $8|(n^2 - 1)$.

Proof. Assume $n = 2a + 1$ for some integer a. Then $n^2 - 1 = (2a+1)^2 - 1 = 4a^2 + 4a = 4a(a+1)$. Notice a and $a + 1$ have different parity. □

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

Proof. We have to prove that 3 divides $(a+b)^3 - a^3 - b^3$ for all $a, b \in \mathbb{Z}$. □

(6) Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod n$ and $a \equiv c \pmod n$, then $c \equiv b \pmod n$.
- $a - b = qn$ for some q. Or $b = a - qn$.
- $a - c = pn$ for some p. Or $c = a - pn$.
- $c - b = a - pn - a + qn = (q - p)n$.

(7) If $a \in \mathbb{Z}$ and $a \equiv 1 \pmod 5$, then $a^2 \equiv 1 \pmod 5$.
- $a - 1 = 5q$ for some q. Or $a = 5q + 1$
- $a^2 = (5q+1)^2 = 25q + 1 + 10q$, or $a^2 - 1 = 5 \cdot 7q$.

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

Proof. Notice $a^3 - b^3 = (a-b)(a^2 + b^2 + ab)$. □

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

Proof. $a - r = qn$. □

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

Proof. $ca - cb = c(a - b)$. □

(11) If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv db \pmod n$.
- $a - b = qn$ and $c - d = pn$ for some integers p, q.
- $a = b + qn, c = d + pn$, and thus $ac = (b+qn)(d+n) = bd + bpn + dqn + pqn^2 = bd + n(bp + dq + pqn)$

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

Proof. (contrapositive) Assume n is not prime. We can write it as $n = pq$ where both $p, q > 1$. Then $2^n - 1 = 2^{pq} - 1$

TODO If $n = 2^k - 1$ for $k \in \mathbb{N}$, then every entry in Row n of Pascal's Triangle is odd.
- $n = 2^k - 1$
- $\binom{n}{j} = (2^k - 1)!/j!/(2^k - 1 - j)! = (2^k - 1)(2^k - 2)...(2^k - j)/j!$
- Looks like there are exactly the same number of factors in numerator and denominator. Let's explore around this idea.
- $2^k - 1$ are odd numbers. Same if we substitute 1 with another odd number.
- $\binom{2^k-1}{0} = 1$.
- $\binom{2^k-1}{1} = 2^k - 1$.
- $\binom{2^k-1}{2} = \frac{(2^k-1)(2^k-2)}{2} = \frac{2(2^k-1)(2^{k-1}-1)}{2} = (2^k - 1)(2^{k-1} - 1)$. Product of two odd numbers.

- $\binom{2^k-1}{3} = \frac{(2^k-1)2(2^{k-1}-1)(2^k-3)}{3\cdot 2} = \frac{1}{3}(2^k-1)(2^k-3)$. More odd stuff. No two's. Notice how similar to the previous case. Also, maybe we could prove on the side that 3 divides $(2^k\text{-}1)(2^k\text{-}3)$.
- $\binom{2^k-1}{4} = \frac{(2^k-1)2(2^{k-1}-1)(2^k-3)(2^k-4)}{4\cdot 3\cdot 2} = \binom{2^k-1}{3}\cdot\frac{2^k-4}{4} = \binom{2^k-1}{3}(2^{k-2}-1)$. A bunch of no-two's! So far, so good.
- $\binom{2^k-1}{5} = \frac{(2^k-1)\cdots(2^k-5)}{5\cdot 4!} = \binom{2^k-1}{4}\frac{2^k-5}{5}$. Hmmm.
- $\binom{2^k-1}{6} = \binom{2^k-1}{5}\frac{2^k-6}{6} = \binom{2^k-1}{5}\frac{2^{k-1}-3}{3}$. Still can't see it through, but almost.
- Back to the 5:
$\binom{2^k-1}{5} = (2^k-1)\cdot\frac{2^k-2}{2}\cdot\frac{2^k-3}{3}\frac{2^k-4}{4}\cdot\frac{2^k-5}{5}$
$= \underbrace{(2^k-1)(2^{k-1}-1)(2^{k-2}-1)}_{\text{bunch of odds}}\frac{2^k-3}{3}\cdot\frac{2^k-5}{5}$.

(13) **DONE** If $a \equiv 0 \pmod 4$ or $a \equiv 1 \pmod 4$, then $\binom{a}{2}$ is even.
- $\binom{a}{2} = (1/2)a!/(a-2)! = a(a-1)/2$
- Case 1: $a = 4b$.
- $\binom{4b}{2} = 2b(4b-1)$, even.
- Case 2: $a = 4b+1$.
- $\binom{4b+1}{2} = (4b+1)2b$. even.

(14) If $n \in \mathbb{Z}$, then 4 does not divide (n^2-3).
  (a) A direct proof with cases:
    - Case 1: If $n \equiv 0 \pmod 4$, then $n^2 \equiv 0 \pmod 4$ as well.
    - Case 2: If $n \equiv 1 \pmod 4$, then $n = 4q+1$ and $n^2 = 16q^2+1+8q$ for some q. This means $n^2 \equiv 1 \pmod 4$.
    - Case 3: If $n \equiv 2 \pmod 4$, then $n = 4q+2$ and $n^2 = 16q^2+4+16q$ for some q. This means $n^2 \equiv 0 \pmod 4$,
    - Case 4: If $n \equiv 3 \pmod 4$, then $n = 4q+3$ and $n^2 = 16q^2+9+8q = 8(2q^2+q+1)+1$ for some q, This means $n^2 \equiv 1 \pmod 4$.
    - We've proven a bunch of things, actually, not only what we were given.
  (b) A proof by contrapositive/contradiction.
    - Assume $n^2 \equiv 3 \pmod 4$.
    - There exists q so that $n^2 = 4q+3 = 2(2q+1)+1$.
    - n^2 is odd.
    - n is odd. $n = 2a+1$ for some a
    - $n^2 = (2a+1)^2 = 4a^2+4a+1 = 4(a^2+a)+1$
    - We have that $4(a^2+a)+1 = 4q+3$
    - $4(a^2+a-q) = 2$ Not possible. n cannot be an integer.

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

(16) **TODO** If $a \equiv b \pmod n$, then $\gcd(a,n) = \gcd(b,n)$.
- Assume WLOG that $a > b$. (if they are equal, nothing to prove)
- There is k that divides a and n but does not divide b and n.
- Write $a = kA, n = kN$
- $a - b = kA - b$.
- $a - b = qn$

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