Chapter 4

Exercise (14). If $n \in \mathbb{Z}$, then $5n^2 + 3n + 7$ is odd. (Try cases.)

Proof. Suppose $n \in \mathbb{Z}$. Then n must be either an even or odd integer.

Case 1: Lets suppose that n is an even integer. Then by the definition of an even integer, n can be expressed as $n = 2k$, where $k \in \mathbb{Z}$. Therefore $5n^2 + 3n + 7 = 5(2k)^2 + 3(2k) + 7 = 20k^2 + 6k + 7 = 2(10k^2 + 3k + 3) + 1 = 2m + 1$, where $m = 10k^2 + 3k + 3$. Note that m is an integer because of the closure properties of the integers. Since $5n^2 + 3n + 7 = 2m + 1$, then $5n^2 + 3n + 7$ an odd integer by the definition of odd. Thus when n is even, then $5n^2 + 3n + 7$ is odd.

Case 2: Suppose that n is an odd integer. Then by the definition of an odd integer, n can be expressed as $n = 2k + 1$, where $k \in \mathbb{Z}$. Therefore $5n^2 + 3n + 7 = 5(2k + 1)^2 + 3(2k + 1) + 7 = 5(4k^2 + 4k + 1) + 6k + 3 + 7 = 20k^2 + 20k + 5 + 6k + 3 + 7 = 20k^2 + 26k + 15 = 2(10k^2 + 13k + 7) + 1 = 2m + 1$, where m $= 10k^2 + 13k + 7$ and likewise $m \in \mathbb{Z}$. Since $5n^2 + 3n + 7 = 2m + 1$, then $5n^2 + 3n + 7$ is odd by definition. Thus when n is odd, then $5n^2 + 3n + 7$ is odd.

In each case $5n^2 + 3n + 7$ is odd, satisfying all possible integer values for n. □

Exercise (16). If two integers have the same parity, then their sum is even. (Try cases.)

Proof. Suppose we have $x, y \in \mathbb{Z}$ such that they share the same parity, that is to say either x and y are both even or x and y are both odd.

Case 1: Suppose x is even and y is even, then they can be express as $x = 2p$ and $y = 2q$ for some $p, q \in \mathbb{Z}$. Therefore $x + y = (2p) + (2q) = 2p + 2q = 2(p + q) = 2n$, where $n = p + q$ and $n \in \mathbb{Z}$ because of the closure properties of addition under the integers. Because $x + y = 2n$, that makes $x + y$ even by definition whenever x and y are even.

Case 2: Suppose x is odd and y is odd, then $x = 2p + 1$ and $y = 2q + 1$ for some $p, q \in \mathbb{Z}$.Therefore $x + y = (2p + 1) + (2q + 1) = 2p + 1 + 2q + 1 = 2p + 2q + 2 = 2(p + q + 1) = 2n$, where $n = p + q + 1$ and $n \in \mathbb{Z}$ because of the closure properties of addition under the integers. Because $x + y = 2n$, our sum $x + y$ is even by definition.

Thus for all cases in which two integers have the same parity, where either both integers are odd or both integers are even, we observe that their sum is even. □

Exercise (18). Suppose x and y are positive real numbers. If $x < y$, then $x^2 < y^2$.

Proof. Suppose $x, y \in \mathbb{R}+$ and that $x < y$. Multiplying both sides of the inequality by x will reveal that $x^2 < yx$. Likewise when we multiply both sides of the inequality by y, we reveal that $xy < y^2$. Note that $xy = yx$ because of the commutative properties of multiplication. Combining our inequality results in $x^2 < xy < y^2$. Hence by the transitivity propety under inequalities in the real numbers, $x^2 < y^2$. Thus for all positive real numbers, if $x < y$ then $x^2 < y^2$. □

Exercise (20). If a is an integer and $a^2 \mid a$, then $a \in \{-1, 0, 1\}$.

Proof. Suppose that $a \in \mathbb{Z}$ such that $a^2 \mid a$. Then by definition of divisibility, there exists a $b \in \mathbb{Z}$ such that $a = a^2$. In order to show that a is in the set of $\{-1, 0, 1\}$, it suffices to show that there exists such a b for each value of a such that $a = a^2b$ is true.

Case 1: Suppose $a = -1$, then via substitution $a = a^2b$ gives us $-1 = (-1)^2b = 1b$, or $-1 = 1b$. If we let $b = -1$ then we find that $a^2 \mid a$ and that $a \in \{-1, 0, 1\}$.

Case 2: Suppose $a = 0$, then $a = a^2b$ holds for any value of b. Note that although the statement holds, the notion that $a^2 \mid a$ for $a = 0$ is undefined.

Case 3: Suppose $a = 1$, then $a = a^2b$ via substitution is $1 = (1)^2b = 1b$. This holds when we

let $b = 1$.

Thus if a is an integer and $a^2 \mid a$, then a is in the set $\{-1, 0, 1\}$. □

Exercise (26). Every odd integer is a difference of two squares.

Proof. Suppose x is an odd integer, then by definition of odd $x = 2k + 1$ for some $k \in \mathbb{Z}$. Hence $x = 2k + 1 = k^2 + 2k + 1 - k^2 = (2k + 1)^2 - k^2 = l^2 - k^2$, where $l = 2k + 1$ and $l \in \mathbb{Z}$ due to the closure properties of the integers. Note that $l^2 - k^2$ is the difference of two squares.

Thus every odd integer is a difference of two squares. □

Exercise (28). Let $a, b, c \in \mathbb{Z}$. Suppose a and b are not both zero, and $c \neq 0$. Prove that $c \gcd(a, b) \leq gcd(ca, cb)$.

Proof. Suppose $a, b, c \in \mathbb{Z}$. Let $d = \gcd(a, b)$, then by definition $d \mid a$ and $d \mid b$. That means $a = dn$ and $b = dm$ for some $n, m \in \mathbb{Z}$. Multiplying both equations by c we obseve that $ca = cdn$ and $cb = cdm$. Thus $cd \mid ca$ and $cd \mid cb$ where cd. Since $\gcd(ca, cb)$ is the greatest common divisor, $cd \leq \gcd(ca, cb)$. Thus $c * \gcd(a, b) \leq \gcd(ca, cb)$. Note that the inequality holds irrespective of whether $c < 0$ or $c > 0$. □

Chapter 5

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

Proof. (By Contraposition) Suppose $a, b, c \in \mathbb{Z}$ such that a divides b. So $b = an$ for some $n \in \mathbb{Z}$. Multiplying both sides by c, $bc = anc = a(ac) = am$, Let $m = $ ac. Note that by the closure properties of the integers, $m \in \mathbb{Z}$. Since $bc = am$, by definition of divisibility $a \mid bc$.

Therefore by contrapositition if a does not divide bc, then a does not divide b. □

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

Proof. (By Contraposition) Assume $x \in \mathbb{R}$ such that $x \geq 0$. Multiplying both sides by $(x+5)$: $x(x+5) = x^2 + 5x \geq 0(x+5) = 0$. Since $x^2 + 5x \geq 0$ if $x \geq 0$. Then by contraposition it must be the case that if $x^2 + 5x < 0$ then $x < 0$. □

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

Proof. (By Contraposition) Let $x \in \mathbb{R}$ such that $x \geq -1$. When we add 1 to both sides, $x + 1 \geq 0$. Further more when we multiply $(x^2 - x)$ to both sides, $(x^2 - x)(x + 1) = x^3 - x^2 + x^2 - x = x^3 - x \geq 0(x^2 - x) = 0$. Thus $x^3 - x \geq 0$ if $x \geq -1$. Hence by contraposition it must be the case that if $x^3 - x > 0$ then $x > -1$. □

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

Proof. (By Contraposition) Suppose $a, b \in \mathbb{Z}$ such that either a is odd or b is odd. Then there are three distinct possibilities, a is odd and b is even, b is odd and a is even, or a and b are both odd.

Case 1: Suppose a is odd and b is even, then by definition of even and odd $a = 2n + 1$ and $b = 2m$ respectively where $n, m \in \mathbb{Z}$. Hence $ab = (2n + 1)(2m) = 4mn + 2m = 2(2mn + m)$ which is even, and $a + b = 2n + 1 + 2m = 2(n + m) + 1$ which is odd. Thus both ab and $a + b$ being even is false.

Case 2: Suppose a is even and b is odd. Then $a = 2n$ and $b = 2m + 1$ for some $n, m \in \mathbb{Z}$. Thus $ab = (2n)(2m+1) = 4mn+2n = 2(2mn+n)$ which is even and $a+b = 2n+2m+1 = 2(n + m) + 1$ which is odd. It is not the case that ab and $a + b$ are both even.

Case 3: Suppose a is odd and b is odd. Then $a = 2n + 1$ and $b = 2m + 1$ for some $n, m \in \mathbb{Z}$. Thus $ab = (2n + 1)(2m + 1) = 4nm + 2n + 2m + 1 = 2(2nm + n + m) + 1$ which is odd, and

$a + b = 2n + 1 + 2m + 1 = 2n + 2m + 2 = 2(n + m + 1)$ which is even. Thus both ab and $a + b$ being even is false.

Therefore if a or b is odd, then ab or $a + b$ is odd. It follows by contrapositition that if ab and $a + b$ are even then a and b are even. □

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

Proof. (By Contraposition) Suppose $n \in \mathbb{Z}$ such that $3 \mid n$. Then by definition of divisibility n can be expressed as $n = 3k$ for some $k \in \mathbb{Z}$. It follows that $n^2 = (3k)^2 = 9k^2 = 3(3k^2) = 3b$, where $b = 3k^2$. Thus $3 \mid n^2$ if $3 \mid n$. By contraposition it follows that if $3 \nmid n^2$ then $3 \nmid n$. □

Exercise (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. (By Contraposition) Let $x, y, z \in \mathbb{Z}$ and $x \neq 0$ such that $x \mid y$ or $x \mid z$. Then $x \mid y$ can be expressed as $y = xa$ for some $a \in \mathbb{Z}$. It follows that $yz = xaz = x(az)$ noting that $az \in \mathbb{Z}$ because of the closure properties of the integers. By definition $x \mid yz$. Similarly if $x \mid z$ then $z = xb$ for some $b \in \mathbb{Z}$ and $yz = xbz = x(bz)$ where $bz \in \mathbb{Z}$. Thus when $x \mid z$ or $x \mid y$ then $x \mid yz$, it follows by contraposition that if $x \nmid yz$ then $x \nmid y$ and $x \nmid z$. □

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

Proof. (By Contraposition) Lets suppose that $x, y \in \mathbb{Z}$ and x and y do not share the same parity, i.e. x is odd and y is even or y is odd and x is even.

Case 1: Suppose x is even and y is odd, then $x = 2n$ and $y = 2k + 1$ for some $n, k \in \mathbb{Z}$. It follows that $x + y = (2n) + (2k + 1) = 2n + 2k + 1 = 2(n + k) + 1$. Thus $x + y$ is odd by definition.

Case 2: Suppose x is odd and y is even, then $x = 2n + 1$ and $y = 2k$ for some $n, k \in \mathbb{Z}$. It fllows that $x + y = (2n + 1) + (2k) = 2n + 2k + 1 = 2(n + k) + 1$. Thus $x + y$ is odd by

definition in this case as well.

Therefore when x and y do not have the same parity, $x + y$ is odd. It follows that by contraposition if $x + y$ is even then x and y must share the same parity. □

Exercise (18). If $a, b \in \mathbb{Z}$, then $(a + b)^3 \equiv a^3 + b^3 \pmod 3$.

Proof. Suppose $a, b \in \mathbb{Z}$, Observe that $(a+b)^3 - (a^3+b^3) = a^3 + 3a^2b + 3ab^2 + b^3 - a^3 - b^3 = 3(a^2b + ab^2)$ Note that $a^2b + ab^2$ is an integer by closure the closure properties of the integers. Thus $3 \mid [(a + b)^3 - (a^3 + b^3)]$, in other words $(a + b)^3 \equiv a^3 + b^3 \pmod 3$. □

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

Proof. Assume $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $a \equiv b \pmod n$ and $a \equiv c \pmod n$. Then there exists an n such that $n \mid (a - b)$ and $n \mid (a - c)$. Then by definition of divisibility, $(a - b) = nx$ and $(a - c) = ny$ for some $x, y \in \mathbb{Z}$. Observe that by subtracting the two equations, $(a - b) - (a - c) = c - b = nx - ny = n(x - y)$. Thus $c - b = n(x - y)$, so $n \mid (c - b)$ by definition of divisibility. Therefore $c \equiv b \pmod n$ by definition of congruence modulo n. □

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

Proof. Suppose $a \in \mathbb{Z}, n \in \mathbb{N}$ such that a has a remainder r when divided by n. By the division algorithm $a = nx + r$, where $x \in \mathbb{Z}$ and $r \in [0, n)$. Consider what happens when we subtract both sides of the equation by the remainder: $a - r = nx + r - r = nx$. So $n \mid (a - r)$ because $a - r = nx$. Therefore $a \equiv r \pmod n$ by definition of congruence modulo n. □

Exercise (24). If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Proof. Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then there exists an $n \in \mathbb{Z}$ such that $a = b + nx$ and $c = d + ny$, where $x, y \in \mathbb{Z}$. It follows that $ac = (b + nx)(d + ny) = bd + bny + dnx + n^2xy = bd + n(by + dx + nxy)$, so $ac = bd + n(by + dx + nxy)$. Subtracting both sides by bd gives $ac - bd = n(by + dx + nxy)$. Therefore $ac \equiv bd \pmod{n}$ by definition of congruence modulo n. □

Exercise (25). Let $n \in \mathbb{N}$. If $2^n - 1$ is prime, then n is prime.

Proof. (By Contraposition) Assume $n \in \mathbb{N}$ and n is not prime. Then n can be expressed as $n = ab$ for some $a, b \in \mathbb{Z}$ and $a, b > 1$. It follows that $2^n - 1 = 2^{ab} - 1 = (2^b - 1)(2^{ab-b} + 2^{ab-2b} + 2^{ab-3b} + ... + 2^{ab-ab})$. Thus $2^n - 1$ is a composite number. Therefore by contraposition it must be the case that if $2^n - 1$ is prime, then n is prime. □

Exercise (32). If $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n.

Proof. Suppose $a \equiv b \pmod{n}$. Then $n \mid a - b$ which can be expressed in the form $a - b = xn$ for some $x \in \mathbb{Z}$. Subsequentially $a = b + xn$ and $b = yn + r$ by rhe division algorithm. Thus $a = b + xn = (yn + r) + xn = yn + xn + r = n(y + x) + r$. So we have $a = n(y + x) + r$ and $b = yn + r$. When we divide both sides by n we see that both a and b share the same remainder. Thus when $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n. □