Problems 1, 2, and 3 are worth 15 points each **(5 points per subproblem).** Problems 4 and 5 are worth 30 points each **(10 points per subproblem)**, for a total of **105 points possible**.

1. The following are from the textbook. (5 points each)

1a. 3.4.29 *Use the quotient-remainder theorem with d = 3 to prove that the square of any integer has the form 3k or 3k + 1 for some integer k.*

According to the quotient-remainder theorem, any integer “n” can be written in one of three forms, for some integer “q”:

Case #1	Case #2	Case #3
$n = 3q$	$n = 3q + 1$	$n = 3q + 2$
$n^2 = (3q)^2$	$n^2 = (3q + 1)^2$	$n^2 = (3q + 2)^2$
$n^2 = 9q^2$	$n^2 = 9q^2 + 6q + 1$	$n^2 = 9q^2 + 12q + 4$
$n^2 = 3(3q^2)$	$n^2 = 3(3q^2 + 2q) + 1$	$n^2 = 3(3q^2 +4q + 1) + 1$
$n^2 = 3k$, where $k = 3q^2$	$n^2 = 3k+1$, $k = 3q^2+2q$	$n^2 = 3k+1$, $k = 3q^2 + 4q +1$
Therefore, our arbitrary n^2 can be expressed in either the form *3k or 3k+1* for some integer ‘k’. Q.E.D.		

1b. 3.4.34 *Given any integer ‘n’, if n>3, could n, n+2, and n+4 all be prime? Prove or give a counterexample.*

By quotient-remainder theorem, for d=3, we can express any n (such that n > 3) in one of three forms, for some integer ‘q’. (Note: Because ‘n’ is greater than 3, q is greater than 1, OR q=1 and n = 4 or n = 5.)

Case #1	Case #2	Case #3
$n = 3q$, $q > 1$	$n = 3q + 1$, $q > 1$	$n = 3q + 2$, $q > 1$
n’ cannot be prime, as it is the product of ‘3’ and ‘q’, both greater than 1.	$n+2 = 3(q+1)$ So n+2 is not prime.	$n+4 = (3q+2)$ So n=4 is not prime.
Case #4	**Case #5**	**So in all five cases, at least one of n, n+2, and n+4 is *not* prime.**
n=4, q = 1	n = 5, q = 1	
n is not prime.	n+4 is not prime.	

1c. 3.4.38 *For any integer $n \geq 1$, n^2+1 has the form $4k+1$ or $4k+2$ for some integer k.*

Direct Proof:

Let ‘n’ be any integer. By parity property, ‘n’ is either even or odd.

Case #1 (n is even)	Case #2 (n is odd)
In this case, $n = 2q$ for some integer q, and so $n^2+1 = (2q)^2 +1 = 4q^2+1$.	By Theorem 3.4.3, there is an integer ‘m’ such that $n^2 +1 = (8m+1)+1 = 4(2m)+2$.
Let $k=q^2$.	Let $k=2m$.
Then ‘k’ is an integer because it is a product of integers, and n^2+1 has the form $4k+1$ for some integer k.	Then k is an integer because it is a product of integers, and thus n^2+1 has the form $4k+2$ for some integer k.
Therefore, for any integer $n \geq 1$, n^2+1 has either the form $4k+1$ or $4k+2$ for some integer k. Q.E.D.	

(This problem could also have been solved by using four cases, as in 3.4.37)

2. The following are from the textbook. (5 points each)

2a. 3.5.17 For all integers *n*,

	n/3	if *n mod 3* = 0
floor(n/3) =	(n-1)/3	if *n mod 3* = 1
	(n-2)/3	if *n mod 3*

Proof: Let ‘n’ be any integer. By quotient-remainder theorem and definition of *mod*, either *n mod* 3 = 0 or *n mod* 3 = 1 or *n mod* 3 = 2.

Case #1 (n mod 3 = 0)	Case #2 (n mod 3 = 1)	Case #3 (n mod 3 = 2)
n = 3q for some integer q, by definition of mod.	n=3q+1 for some integer q.	n=3q+2 for some integer q.
By substitution and algebra, floor(n/3) = floor (3q/3) = floor(q) = q, because q is an integer.	As earlier, floor(n/3) = floor(q+1/3) =q	floor(n/3) = floor((3q+2)/3) = floor (3q/3 + 2/3) =floor(q+2/3) =q
Because n=3q, q = n/3, and therefore floor(n/3) = q = n/3	Solving n=3q+1 for q gives q= (n-1)/3, and so: floor(n/3) = q = (n-1)/3	But q = (n-2)/3 (by solving n=3q+2 for q.) So, floor (n/3) = (n-2)/3
Cases 1,2, and 3 show that no matter what integer ‘n’ is given, floor(n/3) always has one of the three given forms.		

2b. 3.5.18 For all real numbers x and y,

ceiling(x+y) = ceiling(x) + ceiling(y)

False - Counterexample: x=y=1.5

Then,

ceiling(x+y) = ceiling(1.5+1.5) = ceiling(3) = 3.
ceiling(x)+ceiling(y) = ceiling(1.5)+ceiling(1.5) = 2+2 = 4.

So,

ceiling(x+y) ≠ ceiling(x)+ceiling(y) in this case, and statement is false.

2c. 3.5.19 For all real numbers x,

ceiling(x+1) = ceiling(x) + 1

Proof: Let x be an arbitrary real number — then ceiling(x+1) = n for some integer 'n'. By definition of ceiling, $n-1 < x+1 \le n$, and $n-2 < x \le n-1$. And by definition of ceiling, ceiling(x) = n-1. Then, solving for n gives n = ceiling(x) +1 = ceiling(x+1).

3. Prove the following using a method of your choice. (5 points each)

3a. For any integer n, n^2-2 is not divisible by 4.

Direct Proof: *(other solutions possible)*

Case #1 (n divisible by 4)	Case #2 (n not divisible by 4)
n = 4k, for some integer k. (definition of divisibility)	n = 4k+q (for some integer k and q=1,2, or 3) (quotient-remainder theorem)
$n^2 = 16k^2$	$n^2 = 16k^2 + 8kq + q^2$
$n^2 - 2 = 16k^2 - 2$	$n^2 - 2 = 16k^2 + 8kq + q^2 - 2$
$= 4(4k^2) - 2$	$= 16k^2 + 8k - 1$ or $= 16k^2 + 16k + 2$ or $= 16k^2 + 24k + 7$ $n^2 - 2 =$ $= 4(4k^2 + 2k + 1) + 3$ or $= 4(4k^2 + 4k) + 2$ or $= 4(4k^2 + 3k + 1) + 3$
$n^2 - 2$ is not divisible by 4.	*$n^2 - 2$* is not divisible by 4.

In both cases, *$n^2 - 2$* cannot be divisible by 4.

3b. For any prime number a, b, and c, $a^2 - b^2 \neq c^2$

Proof by Contradiction:

Suppose, for contradiction, that we have prime a, b, and c such that $a^2 - b^2 = c^2$.

Then,

$$c^2 = (a-b)(a+b)$$

And $a-b \geq 1$ (because since $a+b \geq 0$ and $c^2 > 0$, a-b must be positive)

Case 1: $(a-b = 1)$

In this case, because both 'a' and 'b' are prime numbers and the only even prime number is 2, the only possible values for 'a' and 'b' are a=3 and b=2.

Then $(a-b)(a+b) = 1*5 = 5 = c^2$, in which case $c = \sqrt{5}$.
This contradicts the supposition that c is prime.

Case 2: $(a-b > 1)$

In this case, $c^2 = (a-b)(a+b)$ where both $(a-b) > 1$ and $(a+b) > 1$. Because 'c' is prime, the only positive factors of 'c' and 1 are 'c' and 1. And then, by the unique factorization theorem, the only positive factors of 'c^2' are 1, c, and c^2.

Because both (a-b) and (a+b) are greater than 1, the only possibility is that both are equal to 'c'. But this implies that $(a-b) = (a+b)$, which implies that $-b = b$, and hence that $b = 0$.

This contradicts the supposition that 'b' is a prime number.

Thus contradiction is reached in both possible cases, and hence the supposition is false and the original statement is true.

3c. If a, b, and c are integers and $a^2 + b^2 = c^2$, then at least one of a and b is even.

Proof by Contradiction:

Suppose not. That is, suppose there exist integers a,b,c such that 'a' and 'b' are both odd and $a^2 + b^2 = c^2$. By definition of odd, $a = 2k_1 + 1$ and $b = 2k_2 + 1$ for some integers k_1, k_2.

Then, by substitution,

$$\begin{aligned} c^2 = a^2 + b^2 &= (2k_1 + 1)^2 + (2k_2 + 1)^2 \\ &= 4k_1^2 + 4k_1 + 1 + 4k_2^2 + 4k_2 + 1 \\ &= 4(k_1^2 + k_1 + k_2^2 + k_2) + 2 \end{aligned}$$

Let $t = k_1^2 + k_1 + k_2^2 + k_2$. Then 't' is an integer because products and sums of integers are integers. Hence $c^2 = 4t + 2$, or (equivalently) $c^2 - 2 = 5t$.

So, by definition of divisibility, $c^2 - 2$ is divisible by 4.

Then,

$$\begin{aligned} c^2 &= 4m + 2 && \text{... for some integer m} \\ &= 2(2m+1) \end{aligned}$$

And so c^2 is even, and 'n' is even (Proposition 3.6.4). Then $n = 2r$ for some integer r.

(continued on next)

Substituting into equation $n^2 - 2 = 4m$ gives:

$4r^2 = 4m+2$
$2r^2 = 2m + 1$

Since r^2 is an integer, this implies that 2m+1 is even, but since 'm' is an integer, 2m+1 is odd. This contradicts Theorem 3.6.2 that no integer is both even and odd.

Hence the supposition is false and original statement holds.

4. *Prove the following using both contraposition and contradiction.* (10 points each)

4a. For all integers, if n^2 is odd, then n is odd.

Proof by Contradiction:

Suppose, for contradiction, that we have an arbitrary integer 'n' such that n^2 is odd and 'n' is even. Since being even implies that 'n' is divisible by 2, we can express 'n' as follows, for some integer k:

$n = 2(k)$

... and n^2, then, may be expressed...

$n^2 = (2(k))^2$
$n^2 = 4(k^2)$
$n^2 = 2(2k^2)$

We have shown, from the supposition that 'n' was even, that 'n^2' must be an integer multiple of two (and thus also even). This contradicts our other assumption, and therefore if n^2 is odd, 'n' cannot be odd (and must, in that case, be even).

Proof by Contraposition:

Proposition: n^2 odd —> n odd
Contrapositive: n not odd —> n^2 not odd

Rewriting the contrapositive, we can say that to not be odd is to be even, which is equivalent to being an integer multiple of two:

$n = 2(k_1)$ —> $n^2 = 2(k_2)$ ... for some integers k_1, k_2

To prove the contrapositive (above), let's assume that we have some arbitrary, even integer 'n'. Then we can write n^2 as follows:

$n^2 = (n)^2$
$= (2k)^2$ ... for some integer k
$= 2(2k^2)$

From the assumption that 'n' was even, we have shown that n^2 must be an integer multiple of 2, and thus also even. We have proved the contrapositive, and therefore the original statement must also hold:

n^2 odd —> n odd

4b. For all integers m and n, if m+n is even then m and n are both even or both odd.

Proof by Contradiction:

Suppose not. That is, suppose there exist integers *m* and *n* such that *m+n* is even and either *m* is even and *n* is odd or *m* is odd and *n* is even. By exercise 19 in Section 3.1, the sum of any even integer and any odd integer is odd. Thus both when *m* is even and *n* is odd and when *m* is odd and *n* is even, the sum *m+n* is odd. This contradicts the supposition that *m+n* is even, hence the supposition is false and the original statement is true.

Proof by Contraposition:

Suppose *m* and *n* are integers such that one of *m* and *n* is even and the other is odd. By exercise 19 of Section 3.1, the sum of any even integer and any odd integer is odd.

Hence *m+n* is odd.

4c. For all integers a, b, and c, if 'a' divides 'b' and does not divide 'c', then 'a' does not divide '(b+c)'.

Proof by Contradiction:

Suppose not. That is, suppose there exist integers a, b, and c such that:

$$a|b \quad \wedge \quad (\sim a|c) \quad \wedge \quad a|(b+c)$$

By definition of divisibility, there exist integers 'r' and 's' such that b = ar and b+c = as.
By substitution, ar + c = as.
Subtracting ar from both sides gives c = as - ar = a (s-r).
But s-r is an integer because 'r' and 's' are integers. Hence, by definition of divisibility, a|c.

This contradicts our supposition that ~(a|c). Hence, supposition is false and statement is true.

Proof by Contraposition:

By De Morgan's law, we must show that for all integers a, b, and c:

$$a \mid (b+c) \quad \longrightarrow \quad \sim(a|b) \quad \vee \quad (a \mid c)$$

But by logical equivalence of p—>qVr and p^~q—>r, it suffices to show that for all integers a,b, and c:

$$a \mid (b+c) \ \wedge \ (a \mid b) \longrightarrow (a \mid c)$$

So suppose a,b,c are integers such that a|(b+c) and (a|b).

By definition of divisibility, b+c = as and b = ar for some integers 's' and 'r'.
By substitution, c = (b+c) - b = as - ar = a(s-r). But s-r is an integer, because it is a difference of integers, and by definition of divisibility, a | c.

5. Prove the following numbers are irrational (10 points each)

5a. $\sqrt{5}$

(General) Proof by Contradiction:

Suppose not. Suppose there exists an integer 'n' such that 'n' is not a perfect square and $\sqrt{n}$ is rational. By definition of rational, there exist integers 'a' and 'b' such that $\sqrt{n}$ = a/b (*a) and b≠0. Without loss of generality, we can assume that 'a' and 'b' have no common divisors (since if they did, we could simply reduce the fraction to find new 'a' and 'b').

Squaring both sides of equation (*a) gives $n = a^2/b^2$, and multiplying by b^2 gives $b^2n = a^2$.

By unique factorization theorem, a,b, and n have representations as products of primes that are unique excluding written order. By the law of exponents, a^2 and b^2 are products of the same prime numbers as 'a' and 'b' respectively, each written twice.

Consequently, each prime factor in a^2 and in b^2 occurs an even number of times. Since 'n' is not a perfect square, some prime factor 'n' occurs an odd number of times (again by law of exponents). It follows that this same prime factor occurs an odd number of times in the product nb^2 *(because all prime factors in b^2 occur an even number of times).*

Since $nb^2 = a^2$, a^2 contains a prime factor occuring an odd number of times, contradicting earlier demonstration that every prime factor of a^2 occurs an even number of times.

Hence, supposition is false and original statement holds.

5b. $\sqrt{2} + \sqrt{3}$

Proof by Contradiction:

Suppose not. Suppose $\sqrt{2} + \sqrt{3}$ is rational. By definition of rational, $\sqrt{2}+\sqrt{3} = a/b$, for some integers 'a' and 'b', $b \neq 0$. Squaring both sides gives:

$$2+2*\sqrt{2}*\sqrt{3}+3 = a^2/b^2$$

Then $2\sqrt{6} = a^2/b^2 - 5$, and $\sqrt{6} = (a^2 - 5b^2)/(2b^2)$. Now $a^2 - 5b^2$ and $2b^2$ are both integers (because products and differences of integers are integers) and $2b^2 \neq 0$ by zero product property.

Therefore, $\sqrt{6}$ is rational by definition of rational. But $\sqrt{6}$ is irrational because it is not a perfect square (see previous), and so a contradiction has been reached.

Hence, supposition is false and original statement is true.

5c. $\log_3(2)$

Proof by Contradiction:

Suppose not. That is, suppose that $\log_3(2)$ is rational.

-By definition of rational, $\log_3(2) = a/b$ for some 'a' and 'b', $b \neq 0$.
Since logarithms are always positive, assume that 'a' and 'b' are positive.

-By definition of logarithm, $3^{a/b} = 2$. Raising both sides to the *b*th power gives:

$$N = \quad 3^a = 2^b \qquad \text{(for appropriate N)}$$

-Since $b \geq 0$, $N > 2^0 = 1$.

-Consider the prime factorization of N. Because $N = 3^a$, the prime factors of N must all be 3.

-On the other hand, because $N = 2^b$, the prime factors of N are all 2.

-This contradicts the unique factorization theorem stating that the prime factors of any integer greater than 1 are unique except for the order in which they are written.

Hence, supposition is false, and $\log_3(2)$ is rational.