1. **(15 points)** *Below are two proofs relating to divisibility of products.*

   (a) **(7 points)** *Determine the sufficient (and if possible necessary) conditions on an integer n for the following statement to be true: "For integers a and b, if $n \nmid ab$, then $n \nmid a$ and $n \nmid b$.". Then state the condition on n and the resulting impliccation as a proposition and prove it.*

   Proposition 1. *Let n be an integer. If a and b are integers such that $n \nmid ab$, then $n \nmid a$ and $n \nmid b$.*

   Proof. We shall prove the contrapositive of this statement: if either $n \mid a$ or $n \mid b$, then $n \mid ab$. We may thus take as our premise the fact that $n \mid a$ or $n \mid b$. WLOG we may assume that, specifically, $n \mid a$. Thus $a = kn$ for some integer k, so $ab = knb = (kb)n$. Since kb is an integer, it thus follows that $n \mid ab$. □

   (b) **(8 points)** *Determine the sufficient (and if possible necessary) conditions on an integer n for the following statement to be true: "For integers a and b, if $n \mid ab$, then either $n \mid a$ or $n \mid b$.". Then state the condition on n and the resulting impliccation as a proposition and prove it.*

   As seen in class this is *not* true when, for instance, $n = 6$, $a =$, and $b = 3$. However, it is true as long as n is not divisible into smaller factors, i.e. if n is prime.

   Proposition 2. *Let n be a prime integer. If a and b are integers such that $n \mid ab$, then $n \mid a$ or $n \mid b$.*

   Proof. Our premise is that $n \mid ab$; thus $ab = kn$ for some integer k. Since these two products of integers are equal, there is a recombination of factors to regroup a product of four factors into each of the two products: that is, we may consider four integers p, q, r, and s such that $ab = pqrs = kn$ such that $pq = a$ and $rs = b$, while $pr = k$ and $qs = n$. Since $qs = n$, it follows that $q \mid n$; but since n is prime, it follows that q is either ± 1 or q is $\pm n$.

   Case I: $q = \pm 1$**.** Then since $qs = n$, $s = \pm n$, so $b = rs = \pm rn$; since r is an integer, $n \mid b$.

   Case II: $q = \pm n$**.** Then $a = pq = \pm pn$; since p is an integer, $n \mid a$. □

2. **(12 points)** *In class we saw a proof that $\sqrt{2}$ is irrational. Here we will explore variations on it.*

   (a) **(8 points)** *Modify the proof of $\sqrt{2}$'s irrationality to produce a proof that for integer n, $\sqrt{n}$ is irrational if n is not exactly the square of some integer.*

   This one is actually quite difficult. We start by considering n as a product of a square and a factor free of squares: i.e. $n = m^2 r$, where no integer square other than 1 divides r. Since n is not exactly a square, $r > 1$. We can now adapt a lemma from the lecture:

   Lemma 1. *For an integer n and integer r such that no square other than 1 divides r, $r \mid n^2$ if and only if $r \mid n$.*

   Proof. The implication in one direction is easy: if $r \mid n$, then n is equal to rk for some integer k, so $n^2 = (rk)^2 = r(rk^2)$, so n^2 is also divisible by r.

   In the opposite direction, however, we are given that $r \mid n^2$. Since r has no square factors, it is a product of distinct primes $p_1 p_2 p_3 \dots p_\ell$. Thus $n \cdot n = p_1 p_2 \cdots p_\ell k$ for some integer k.

Since any two equal multiplications of integers can be broken down into prime terms and recombined, then there must be a decomposition of $n^2 = abcd$ with a, b, c, and d positive integers such that $ab = n$, $cd = n$, $ac = p_1 \cdots p_\ell$, and $bd = k$. We shall specifically focus on the fact that $ac = p_1 \cdots p_\ell$: since each p_i is prime, either a or c is divisible by each p_i, so since $ab = n$ and $cd = n$, it will follow that each $p_i \mid n$, so $r \mid n$. □

We can then adapt the argument for $\sqrt{2}$ almost exactly:

Theorem 1. *For an integer n not a perfect square, the square root of n is irrational.*

Proof. The statement could be rephrased as an explicit implication: if $x^2 = n$, then x is irrational. Let us proceed by contradiction, and take as our premise the statement that $x^2 = n$ and x is not irrational (i.e., x is rational). We may determine integers m and r such that $n = m^2 r$, where no integer square other than 1 divides r; since n is not a perfect square, $r > 1$. Then, by the definition of a rational number, x may be expressed as a fraction $\frac{p}{q}$ in lowest terms; that is, $x = \frac{p}{q}$ where p and q are integers sharing no divisors greater than 1. Since $m^2 r = x^2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}$, we may see that $p^2 = rm^2q^2$. Thus $r \mid p^2$, and from the above lemma $r \mid p$; let $p = rk$. Then $(rk)^2 = rm^2q^2$, which simplifies algebraically to $rk^2 = m^2q^2$. Thus $r \mid q^2$, so $r \mid p$. However, since both p and q are divisible by r, our presumption that $\frac{p}{q}$ is in lowest terms is directly contradicted. □

(b) **(4 points)** *Explain why this proof couldn't be modified to prove that $\sqrt{4}$ is irrational. Don't merely point out that $\sqrt{4}$ is rational; exhibit why the specific proof of the irrationality of $\sqrt{2}$ doesn't work when the 2 is replaced with a 4.*

The original proof does not yield an easy adaptation because the assertion "$4 \mid n^2$ if and only if $4 \mid n$" is not true in general (e.g. for $n = 6$), and could not replace the similar assertion about the number 2 (which *is* true) in the original proof. If we tried to run 4 through our proof above, we would get that $r = 1$, which would not present a problem until the end, where the assertion that both p and q are divisible by r would not contradict our assertion that $\frac{p}{q}$ was in lowest terms.

3. **(7 points)** *Let $a, b \in \mathbb{Z}$. Prove that if $a^2 + 2b^2 \equiv 0 \pmod 3$, then either a and b are both congruent to zero modulo 3 or neither is congruent to zero modulo 3.*

Proof. We shall prove the contrapositive: if a and b are *not* either both congurent to zero or both noncongruent to zero, then $a^2 + 2b^2 \not\equiv 0 \pmod 3$. Thus, one is congruent to zero and the other is not congruent to zero. Which one is which is not given, so we proceed with a casewise analysis:

Case I: $a \equiv 0 \pmod 3$ **and** $b \not\equiv 0 \pmod 3$**.** Alternatively, $3 \mid a$ and $3 \nmid b$. Using the lemma from the previous question (or an arbitrary-prime version of the one used in class), we can see $3 \mid a^2$ and $3 \nmid b^2$; furthermore, since 2 is prime and not a divisor of 3, we can see that $3 \nmid 2b^2$. Thus $a^2 \equiv 0 \pmod 3$ and $2b^2 \not\equiv 0 \pmod 3$, so by additivity of modular arithmetic, we can see that $a^2 + 2b^2 \not\equiv 0 \pmod 3$.

Case I: $a \not\equiv 0 \pmod 3$ **and** $b \equiv 0 \pmod 3$**.** Alternatively, $3 \nmid a$ and $3 \mid b$. Using the lemma from the previous question (or an arbitrary-prime version of the one used in class), we can see $3 \nmid a^2$ and $3 \mid b^2$; furthermore, we can see easily that $3 \mid 2b^2$. Thus $a^2 \not\equiv 0 \pmod 3$ and $2b^2 \equiv 0 \pmod 3$, so by additivity of modular arithmetic, we can see that $a^2 + 2b^2 \not\equiv 0 \pmod 3$. □

4. **(6 points)** *Let A, B, and C be sets. Prove that $(A - B) \cup (A - C) = A - (B \cap C)$.*

   Proof. We shall first prove that $(A-B)\cup(A-C) \subseteq A-(B\cap C)$. Consider $x \in (A-B)\cup(A-C)$. By the definition of a union, we know that either $x \in A - B$ or $x \in A - C$. We shall analyze each case:

   Case I: $x \in A - B$**.** Then $x \in A$ and $x \notin B$. Since $x \notin B$, it follows that $x \notin B \cap C$. Thus, since $x \in A$ and $x \notin B \cap C$, we can conclude that $x \in A - (B \cap C)$.

   Case II: $x \in A - C$**.** Then $x \in A$ and $x \notin C$. Since $x \notin C$, it follows that $x \notin B \cap C$. Thus, since $x \in A$ and $x \notin B \cap C$, we can conclude that $x \in A - (B \cap C)$.

   Since an arbitrary element of $(A - B) \cup (A - C)$ has been shown to be in $A - (B \cap C)$, we may conclude that $(A - B) \cup (A - C) \subseteq A - (B \cap C)$.

   Now let us prove that $A-(B\cap C) \subseteq (A-B)\cup(A-C)$. Consider $y \in A-(B\cap C)$. Thus $y \in A$ but $y \notin B \cap C$. In order for y to not be an element of $B \cap C$, it must fail to be an element of either B or C. We can investigate both possibilities casewise:

   Case I: $y \notin B$**.** Then, together with the previously seen fact that $y \in A$, we may conclude that $y \in (A - B)$, and thus $y \in (A - B) \cup (A - C)$.

   Case I: $y \notin C$**.** Then, together with the previously seen fact that $y \in A$, we may conclude that $y \in (A - C)$, and thus $y \in (A - B) \cup (A - C)$. □

5. **(4 point bonus)** *Prove (possibly following the structure of the similar proof in class) that if every two vertices of a regular 17-sided polygon are joined with segments colored red, green, or blue, then regardless of how the segments are colored, some three vertices are joined by three edges of the same color.*

   Proof. Let us pick an arbitrary vertex of our 17-gon, and label it x; now let us consider the 16 segments emenating from this vertex to every other vertex of the polygon; each segment has been colored red, green, or blue. Of the three colors, it is impossible that they all appear 5 or fewer times among these 16 segments; that could only color 15 segments. Thus, 6 of these segments with one endpoint at x must be the same color; WLOG we can presume that color is red. Let us then name these six red segments' other endpoints $y_1, y_2, y_3, y_4, y_5, y_6$.

   There are two cases to be dealt with as we inspect the edges among the vertices $y_1, \ldots, y_6$; either the color red is present among these edges or it is not.

   Case I: the segment between some y_i and y_j is red. Then x, y_i, and y_j are mutually connected by red segments.

   Case II: all of the segments among $y_1, \ldots, y_6$ are blue or green. Then we are drawing segments among 6 points in two colors; by the result seen in class, a monochromatic triangle must be produced. □

   The field from which this question (and the 6-vertex example given in class) are drawn is called *Ramsey Theory*, which deals with the monochromatic substructures which must arise when a large structure is colored.

> Die ganzen Zahlen hat der liebe Gott gemacht; alles andere ist Menschenwerk. [The good Lord created the natural numbers; all else is the work of man.]
>
> —attributed to Leopold Kronecker