Homework 1

Madilyn Simons

1. **a** We can prove the statement by induction. First, let $n = 1$. As such, $n^2 = 1$. By the Division Algorithm, $n^2 = 8 \cdot 0 + 1$. Thus, the statement holds for $n = 1$. Next, assume the statement holds for $1, 3, 5, ..., n$. Since n is odd, the next consecutive odd number is $n + 2$. Because n^2 leaves a remainder of 1 when divided by 8, let $n^2 = 8 \cdot k + 1$ for some integer k. As such, $(n + 2)^2 = n^2 + 4 \cdot n + 4 = 8k + 4n + 1$. Therefore, $(n + 2)^2$ leaves a remainder of 1 when divided by 8. By induction, for any odd number n, n leaves a remainder of 1 when divided by 8.

   b Let $n = 2^{a_0} \cdot {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot ... \cdot {p_k}^{a_k}$ be the prime factorization of n such that p_i are distinct prime numbers for all i and there is no i such that $p_i = 2$. As such, $n^2 = 2^{2a_0} \cdot {p_1}^{2a_1} \cdot {p_2}^{2a_2} \cdot ... \cdot {p_k}^{2a_k}$. Since p_i is odd for all i (since all p_i are primes and do not equal 2), ${p_1}^{a_1} \cdot {p_2}^{a_2} \cdot ... \cdot {p_k}^{a_k}$ is also odd. By $1a$, ${p_1}^{2a_1} \cdot {p_2}^{2a_2} \cdot ... \cdot {p_k}^{2a_k}$ leaves a remainder of 1 when divided by 8. Let ${p_1}^{2a_1} \cdot {p_2}^{2a_2} \cdot ... \cdot {p_k}^{2a_k} = 8b + 1$ for some integer b. Thus, $n^2 = 2^{2a_0} \cdot (8b + 1) = 4^{a_0} \cdot (8b + 1) = 8 \cdot (4^{a_0} b) + 4^{a_0}$. Since multiples of 4 can only leave a remainder of either 0 or 4 when divided by 8 ($4(2k) = 8k$ and $4(2k + 1) = 8k + 4$ for all integers k) and $n^2 = 8 \cdot (4^{a_0} b) + 4^{a_0}$, n^2 can only leave a remainder or 0 or 4 when divided by 8.

2. If $3 \nmid n$, then, by the Division Algorithm, either $n = 3k+1$ or $n = 3k+2$ for some integer k. First, assume $n = 3k + 1$. Thus, $n^2 - 1 = (3k + 1)^2 - 1 = 3 \cdot (3k^2 + 2k)$. Therefore, $3|(n-1)^2$ for this case. Next, assume $n = 3k+2$. Thus, $n^2 - 1 = (3k + 2)^2 - 1 = 3 \cdot (3k^2 + 4k + 1)$. Therefore, $3|(n - 1)^2$ for all n such that $3 \nmid n$.

3. Let $a = {p_1}^{x_1} \cdot ... \cdot {p_k}^{x_k}$ and $b = {p_1}^{y_1} \cdot ... \cdot {p_k}^{y_k}$ be the prime factorizations of a and b respectively such that $x_i \geq 0$ and $y_i \geq 0$ for all $i \leq k$. Let $c = {q_1}^{z_1} \cdot ... \cdot {q_j}^{z_j}$ be the prime factorization of c given there are no m, n such that $p_m = q_n$. This holds because $(a, c) = 1$ and $(b, c) = 1$, meaning a and c have no common prime factors and b and c have no common prime factors. Thus, $ab = {p_1}^{x_1+y_1} \cdot ... \cdot {p_k}^{x_k+y_k}$. Therefore, ab and c also do not have any common prime factors. This implies that $(ab, c) = 1$.

4. Either $(a, b) = 1$ or $(a, b) \neq 1$. First, suppose $(a, b) = 1$. Since a and b do not have any common prime factors, c must be a multiple of ab in order to be divisible by both a and b. Next suppose $(a, b) \neq 1$. Let $a = {p_1}^{x_1} \cdot ... \cdot {p_k}^{x_k}$ and $b = {p_1}^{y_1} \cdot ... \cdot {p_k}^{y_k}$ be the prime factorizations of

a and b respectively such that $x_i \geq 0$ and $y_i \geq 0$ for all $i \leq k$. If a and b both divide c, then $m = {p_1}^{max(x_1,y_1)} \cdot ... \cdot {p_k}^{max(x_k,y_k)}$ is a factor of c. If $(a,b) = {p_1}^{min(x_1,y_1)} \cdot ... \cdot {p_k}^{min(x_k,y_k)}$, then $m \cdot (a,b) = ab$. Let $c = m \cdot x$ for some integer x. Thus, $c = m \cdot x \cdot (a,b) = a \cdot b \cdot x$ is divisible by ab.

5. If $(a,6) = 1$, then either $a = 6x+1$ or $a = 6x-1$ for some integer x (since $(k,6) > 1$ for all $2 \leq k \leq 4$). Similarly, either $b = 6y+1$ or $b = 6y-1$. Suppose $a = 6x+1$. Consequently, $a^2 = 36x^2+12x+1 = 12x(3x+1)+1$. Either x is even or odd. First, assume x is even, so $x = 2k$ for some integer k. Therefore, $a^2 = 24k(6k+1)+1$, which leaves a remainder of 1 when divided by 24. If x is odd, then $x = 2k+1$ for some integer k. As such, $a^2 = 24(6k^2+7k+2)+1$, which also leaves a remainder of 1 when divided by 24. Next, suppose $a = 6x-1$. By the same logic as before, $a^2 = 24k(6k-1)+1$ when x is even and $a^2 = 24(6k^2+5k+1)+1$ when x is odd, both of which leave a remainder of 1 when divided by 24. Therefore, a^2 always leaves a remainder of 1 when divided by 24. By the same logic, b^2 also always leaves a remainder of 1 when divided by 24. Let $a^2 = 24m+1$ and $b^2 = 24n+1$ for some integers m,n. Therefore, $a^2 - b^2 = (24m+1) - (24n+1) = 24(m-n)$, which is divisible by 24.

6. First, assume n is a square number. If $n = {p_1}^{a_1} \cdot ... \cdot {p_k}^{a_k}$, then $\sqrt{n} = {p_1}^{a_1/2} \cdot ... \cdot {p_k}^{a_k/2}$. By the definition of prime factorization, a_i and $a_i/2$ must be integers for all i such that $1 \leq i \leq k$. Thus, $a_i/2$ can only be an integer if 2 evenly divides a_i. Therefore, each a_i must be even. Next, assume each a_i is even. Let $a_i = 2b_i$ for some integers b_i. Thus, $n = {p_1}^{2b_1} \cdot ... \cdot {p_k}^{2b_k}$. Since each b_i is an integer, $\sqrt{n} = {p_1}^{b_1} \cdot ... \cdot {p_k}^{b_k}$ is an integer and n must be a square number.

7. Let $a = {p_1}^{x_1} \cdot ... \cdot {p_k}^{x_k}$ and $b = {q_1}^{y_1} \cdot ... \cdot {q_j}^{y_j}$ be the prime factorizations of a and b respectively such that $p_m \neq q_n$ for all m,n. As such, $ab = {p_1}^{x_1} \cdot ... \cdot {p_k}^{x_k} \cdot {q_1}^{y_1} \cdot ... \cdot {q_j}^{y_j}$. If ab is a square, then $x_1,...,x_k$ and $y_1,...,y_j$ must be even. Because $x_1,...,x_k$ are even, a must a square. Similarly, since $y_1,...,y_j$ are even, b must also be a square.