CSE 16
Winter 2022
Quiz 4 **Solutions**

1. (20 Points) Let $n \in \mathbb{Z}$. Prove that $n^2 \not\equiv 2 \pmod{3}$.

   Proof:
   Every $n \in \mathbb{Z}$ has one of three possible remainders upon division by 3, namely 0, 1 or 2. Therefore each $n \in \mathbb{Z}$ satisfies exactly one of $n \equiv 0 \pmod{3}$, $n \equiv 1 \pmod{3}$ or $n \equiv 2 \pmod{3}$. We have three cases to consider.

   Case 0: $n \equiv 0 \pmod{3}$
   In this case $n = 3k$ (for some $k \in \mathbb{Z}$), so $n^2 = 9k^2 = 3(3k^2)$, whence $3|n^2$, and $n^2 \equiv 0 \pmod{3}$.

   Case 1: $n \equiv 1 \pmod{3}$
   In this case $n = 3k + 1$ (for some $k \in \mathbb{Z}$), therefore $n^2 = (3k + 1)^2 = 3(3k^2 + 2k) + 1$, showing that $n^2 \equiv 1 \pmod{3}$.

   Case 2: $n \equiv 2 \pmod{3}$
   In this case $n = 3k + 2$ (for some $k \in \mathbb{Z}$), and $n^2 = 3(3k^2 + 4k + 1) + 1$. Again $n^2 \equiv 1 \pmod{3}$.

   In *no case* do we have $n^2 \equiv 2 \pmod{3}$. Since these cases exhaust all possibilities, we have established that $n^2 \not\equiv 2 \pmod{3}$ for any $n \in \mathbb{Z}$. ■

2. (30 Points) Let $a, b, c \in \mathbb{Z}$. Suppose $a|bc$ and $\gcd(a, b) = 1$. Prove that $a|c$. (Hint: use the following theorem proved in class: $\gcd(a, b) = an + bm$ for some $n, m \in \mathbb{Z}$.)

   Proof:
   Since $a|bc$ we have $bc = ka$ for some $k \in \mathbb{Z}$. Since $\gcd(a, b) = 1$, the hint gives us

   $$1 = an + bm$$

   for some $n, m \in \mathbb{Z}$. Multiplying this equation by c, yields

   $$c = acn + bcm.$$

   By using $bc = ka$, the above equation above becomes

   $$c = acn + kam = a(cn + km).$$

   Since $cn + km \in \mathbb{Z}$, we have $a|c$, as claimed. ■