Steven Rosendahl
Homework 1

1. What are the possible remainders when a perfect square is divided by 3 or by 6?

   Let $k \in \mathbb{Z}$ such that $a = k^2$. By the division algorithm, we have that

   $$k = 3q_1 + r_1 \qquad \text{and} \qquad k = 6q_2 + r_2.$$

   case $k = 3q_1 + r_1$: Squaring k yields

   $$k^2 = 9q_1^2 + 6q_1r_1 + r_1^2.$$

   Since $k^2 = a$, we have that

   $$\begin{aligned} a &= 3(3q_1^2 + 2q_1r_1) + r_1^2 \\ &= 3q_0 + r_0, \text{ where } q_0 = (3q_1^2 + 2q_1r_1) \text{ and } r_0 = r_1^2. \end{aligned}$$

   We know by the division algorithm that $r_0 \in \{0, 1, 2\}$. If we let $r_0 = 0$ or $r_0 = 1$, then $r_1^2 < 4$ and still in $\{0, 1, 2\}$. Therefore, 0 and 1 are possible remainders. If we let $r_0 = 2$, then $r_1^2 = 4$, which is not less than 4. However, we have that

   $$\begin{aligned} a &= 3q_0 + 2^2 \\ &= 3q_0 + 4 \\ &= 3q_0 + 3 + 1 \\ &= 3(q_0 + 1) + 1, \end{aligned}$$

   Which implies that 1 is a valid remainder. Therefore, 0 and 1 are the only valid remainders.

   case $k = 6q_2 + r_2$: If we square k, then we have

   $$k^2 = 36q_2^2 + 12q_2r_2 + r_2^2.$$

   Since $a = k^2$, we have that

   $$\begin{aligned} a &= 36q_2^2 + 12q_2r_2 + r_2^2 \\ &= 6(6q_2^2 + 2q_2r_2) + r_2^2 \\ &= 6q_0 + r_0, \text{ where } q_0 = 6q_2^2 + 2q_2r_2 \text{ and } r_0 = r_2^2. \end{aligned}$$

   We know that for $r_0 = 0, 1,$ and 2, $r_2^2 \leq 6$, so they are valid remainders. For $r_0 = 3, 4,$ and 5, we have

   $r_0 = 3$

   $$\begin{aligned} a &= 6q_0 + 9 \\ &= 6q_0 + 6 + 3 \\ &= 6(q_0 + 1) + 3 \end{aligned}$$

   $\therefore$ 3 is a valid remainder.

   $r_0 = 4$

   $$\begin{aligned} a &= 6q_0 + 16 \\ &= 6q_0 + 12 + 4 \\ &= 6(q_0 + 2) + 4 \end{aligned}$$

   $\therefore$ 4 is a valid remainder.

   $r_0 = 5$

   $$\begin{aligned} a &= 6q_0 + 25 \\ &= 6q_0 + 24 + 1 \\ &= 6(q_0 + 4) + 1 \end{aligned}$$

   $\therefore$ 1 is a valid remainder.

   Therefore, the valid remainders are $\{0, 1, 2, 3, 4\}$.

   $\triangle$

2. Suppose $a, b, c, d \in \mathbb{Z}$ are such that $a|b$ and $c|d$. Prove that $ac|bd$.

   Since $a|b$, we have that $b = an$ for some $n \in \mathbb{Z}$. We also have that $c|d$, so $d = cm$ for some $m \in \mathbb{Z}$. The product $bd = (an)(cm)$, which, after rearranging, yields $bd = (nm)(ac)$. We know that $nm \in \mathbb{Z}$, so we let $j = nm$. Then $bd = jac$, so $ac|bd$.

$\triangle$

3. Suppose $a, b, m \in \mathbb{Z}$ and $m \neq 0$. Prove that $a|b$ if and only if $ma|mb$.

   Suppose $a|b$. Then $b = na$ for some $n \in \mathbb{Z}$. Multiplying both sides of the equation yields $mb = mna$; therefore $ma|mb$.
   Suppose $ma|mb$, and $m \neq 0$. Then $mb = mna$ for some $n \in \mathbb{Z}$. We know that $\frac{m}{m} = 1$, so dividing both sides by m gives us $b = na$. Therefore $a|b$.

$\triangle$

4. Suppose $a, b \in \mathbb{Z}$ with $b \neq 0$ and $a|b$. Prove that $|a| \leq |b|$.