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 $ac|bd$.

△

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 $a|b$.

△

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

   Since $a|b$, we have that $b = an$ for some $n \in \mathbb{Z}$. We first need to show that $n \neq 0$. Since $b \neq 0$, $an \neq 0$. Therefore both a and n must not be equal to 0. If we apply the absolute value to b, we have that $|b| = |an|$. We know that $|an| = |a||n|$. Since $n \neq 0$, $|n| \geq 1$. We also know that $|a| \geq 1$, since $a \neq 0$. Therefore $|a||n| \geq |a|$, or $|an| \geq |a|$. Since $|b| = |an|$, we have that $|a| \leq |b|$.

△

5. Suppose that $a, b, c, d \in \mathbb{Z}$ are such that $a|b$ and $c|d$. Does $a + c$ necessarily divide $b + d$?

   Assume $a + c$ divides $b + d$. Let $a = 1$ and $c = -1$. Both 1 and -1 divide all elements of $\mathbb{Z}$, but $1 + -1 = 0$, and 0 does not divide anything. Therefore by counterexample it does not.

△

6. Suppose that $b \in \mathbb{Z}$.

   (a) If $4|b^2$, prove that $2|b$.

   Assume that $4|b^2$ but $2 \nmid b$. Then $b = 2n + r$ for some n and r in $\mathbb{Z}$. We know that $r \neq 0$, and that $0 < r < 2$. Therefore $r = 1$. If we square both sides, we get

$$\begin{aligned} b^2 &= (2n+1)^2 \\ &= 4n^2 + 4n + 1 \\ &= 4(n^2 + n) + 1. \end{aligned}$$

   Therefore $4 \nmid b$, since it has a remainder of 1.

   (b) If $9|b^2$, prove that $3|b$.

   Assume that $9|b^2$, but $3 \nmid b$. Then $b = 3n + r$ where n and r and in $\mathbb{Z}$, and $0 < r < 3$. If we let $r = 1$, then we have

$$\begin{aligned} b &= 3n + 1 \\ b^2 &= (3n+1)^2 \\ &= 9n^2 + 6n + 1 \\ &= 3(3n^2 + 2n) + 1. \end{aligned}$$

   Therefore $3 \nmid b^2$, and since 3 is a factor of 9, $9 \nmid b^2$.

   △

7. Use the Euclidian Algorithm to calculate $gcd(1485, 1745)$.

$$
\begin{aligned}
1745 &= 1485(1) + 260 \\
1485 &= 260(5) + 185 \\
260 &= 185(1) + 75 \\
185 &= 75(2) + 35 \\
75 &= 35(2) + 5 \\
35 &= 5(7) + 0
\end{aligned}
$$

Therefore $gcd(1485, 1745) = gcd(5, 0) = 5$.

8. Suppose that a and b are positive integers. Prove that $gcd(a, b) = a$ if and only if $a|b$.

   Assume that $gcd(a, b) = a$. Then a is a divisor of both a and b by the definition of the gcd. Therefore $a|b$.
   Assume that $a|b$. We know that $a|a$, so a is the greatest integer that divides a. Since $a|b$, we know that a is also a factor of b. If $a < b$, then a is the largest integer that divides both a and b. Therefore $gcd(a, b) = a$. If $a = b$, then a is still the greatest common factor between a and b. Therefore $gcd(a, b) = a$.

△