Solutions to homework 2:

1. Let $a, b \in \mathbb{Z}$. Prove that if ab is odd, then a and b are both odd.

   Proof by Contrapositive: Let $a, b \in \mathbb{Z}$. If a or b are even then ab must be even.

   - **Case 1:** Assume that a is even. Then a must be of the form $2k$ for some $k \in \mathbb{Z}$. Consider the expression ab, so under the assumption that a is even

   then $ab = 2kb$, factoring 2 we see that $2kb = 2(kb)$. Since the product of two integers is an integer, we see that $2(kb) = 2i$ for some $i \in \mathbb{Z}$. Hence, ab is of the form $2i$, thus ab is even.

   - **Case 2:** Consider the first case, without loss of generality.

   Hence by contrapositive, if ab is odd, then a and b are both odd.

   ■

2. Prove that if $a \in \mathbb{Z}$, then $4 \nmid a^2 - 3$.

   Proof: Consider the cases $a \equiv 0 \pmod 4$, $a \equiv 1 \pmod 4$, $a \equiv 2 \pmod 4$, and $a \equiv 3 \pmod 4$.

   - **Case 1:** Assume that $a \equiv 0 \pmod 4$. Then $a^2 - 3 \equiv 0^2 - 3 \pmod 4$. Thus, $a^2 - 3 \equiv -3 \pmod 4$.
   - **Case 2:** Assume that $a \equiv 1 \pmod 4$. Then $a^2 - 3 \equiv 1^2 - 3 \pmod 4$. Thus, $a^2 - 3 \equiv -2 \pmod 4$.
   - **Case 3:** Assume that $a \equiv 2 \pmod 4$. Then $a^2 - 3 \equiv 2^2 - 3 \pmod 4$. Thus, $a^2 - 3 \equiv 1 \pmod 4$.
   - **Case 4:** Assume that $a \equiv 3 \pmod 4$. Then $a^2 - 3 \equiv 3^2 - 3 \pmod 4$. Thus, $a^2 - 3 \equiv 2 \pmod 4$.

   Hence by the previous cases, if $a \in \mathbb{Z}$ then $4 \nmid a^2 - 3$

   ■

3. Let x be a positive real number. Prove that if $2x - \frac{1}{x} > 1$, then $x > 1$.

   Proof: Assume that $2x - \frac{1}{x} > 1$ and x is a positive real number.

$$
\begin{aligned}
2x - \frac{1}{x} &> 1 \\
2x^2 - 1 &> x \\
2x^2 - x - 1 &> 0 \\
(2x+1)(x-1) &> 0
\end{aligned}
$$

   Under the assumption that x must be a positive real number, we know that $(2x + 1)$ must be positive so we can multiply it out leaving the expression $x - 1 > 0$. Hence, $x > 1$.

   ■

4. Let $x \in \mathbb{R}$. Then, prove that $x^2 + |x-6| > 5$.

   Proof:

   Consider:

$$|x-6| = \begin{cases} x-6 & \text{if } x \geq 6 \\ -x+6 & \text{if } x < 6 \end{cases}$$

- **Case 1:** Let $x \in \mathbb{R}$ and assume that $x < 6$. Now consider the fact that $x^2 \geq 0$.

$$\begin{aligned} x^2 &\geq 0 \\ x^2 + 1 &> 0 \\ x^2 - x + 1 &> 0 \\ x^2 - x + 6 - 5 &> 0 \\ x^2 - x + 6 &> 5 \\ x^2 + |x-6| &> 5 \end{aligned}$$

- **Case 2:** Let $x \in \mathbb{R}$ and assume that $x \geq 6$. Now consider the fact that $x^2 \geq 0$.

$$\begin{aligned} x^2 &\geq 0 \\ x^2 + x &> 0 \\ x^2 + x - 11 &> 0 \\ x^2 + x - 6 &> 5 \\ x^2 + |x-6| &> 5 \end{aligned}$$

Hence, If $x \in \mathbb{R}$ then $x^2 + |x-6| > 5$

■

5. Let $n \in \mathbb{Z}$. Prove that if 5 is not a factor of $(n^2-1)(n^2-4)$ then $5|n$.

   Proof by Contrapositive: Let $n \in \mathbb{Z}$. If $5 \nmid n$ then 5 is a factor of $(n^2-1)(n^2-4)$.

- **Case 1:** Assume that $n \equiv 1 (\bmod 5)$. So, when $n \equiv 1 (\bmod 5)$ then $(n^2-1)(n^2-4) \equiv 0 (\bmod 5)$. Thus, 5 is a factor of $(n^2-1)(n^2-4)$ when $n \equiv 1 (\bmod 5)$.

- **Case 2:** Assume that $n \equiv 2 (\bmod 5)$. So, when $n \equiv 2 (\bmod 5)$ then $(n^2-1)(n^2-4) \equiv 0 (\bmod 5)$. Thus, 5 is a factor of $(n^2-1)(n^2-4)$ when $n \equiv 2 (\bmod 5)$.

- **Case 3:** Assume that $n \equiv 3 (\bmod 5)$. So, when $n \equiv 3 (\bmod 5)$ then $(n^2-1)(n^2-4) \equiv 40 (\bmod 5) \equiv 0 (\bmod 5)$. Thus, 5 is a factor of $(n^2-1)(n^2-4)$ when $n \equiv 3 (\bmod 5)$.

- **Case 4:** Assume that $n \equiv 4 (\bmod 5)$. So, when $n \equiv 4 (\bmod 5)$ then $(n^2-1)(n^2-4) \equiv 160 (\bmod 5) \equiv 0 (\bmod 5)$. Thus, 5 is a factor of $(n^2-1)(n^2-4)$ when $n \equiv 4 (\bmod 5)$.

Hence, 5 is a factor of $(n^2-1)(n^2-4)$ when $5 \nmid n$.

■

6. Let $x, y \in \mathbb{Z}$. Prove that $3 \nmid (x^3 + y^3)$ if and only if $3 \nmid (x + y)$.

   Proof:

   - **Case 1:** Proof by contrapositive. Let $x, y \in \mathbb{Z}$. If $3 \mid (x^3 + y^3)$ then $3 \mid (x + y)$. Assume that $3 \mid (x^3 + y^3)$ such that $(x^3 + y^3) \equiv 0 (\bmod 3)$ and consider the following.

     $$\begin{aligned}(x^3 + y^3) &= (x+y)^3 - 3xy(x+y)\\ (x^3 + y^3) &\equiv (x+y)^3 - 3xy(x+y) (\bmod 3)\\ (x+y)^3 - 3xy(x+y) &\equiv 0 (\bmod 3)\end{aligned}$$

     Since $-3xy(x+y) \equiv 0 (\bmod 3)$, then $(x+y)^3 \equiv 0(\text{mod})3$.

     $$\begin{aligned}(x+y)^3 &\equiv 0 (\bmod 3)\\ (x+y) &\equiv 0 (\bmod 3)\\ x+y &\equiv 0 (\bmod 3)\end{aligned}$$

     Thus by by contrapositive, if $3 \mid (x^3 + y^3)$ then $3 \mid (x + y)$.

   - **Case 2:** Proof by contrapositive. Let $x, y \in \mathbb{Z}$. If $3 \mid (x + y)$ then $3 \mid (x^3 + y^3)$. Assume that $3 \mid (x + y)$ such that $(x + y) = 3\ell$ and consider the following.

     $$\begin{aligned}(x^3 + y^3) &= (x+y)^3 - 3xy(x+y)\\ (x+y)^3 - 3xy(x+y) &= (3\ell)^3 - 3xy(3\ell)\\ (3\ell)^3 - 3xy(3\ell) &= 3(9\ell^3 - xy(3\ell))\end{aligned}$$

     Since the product and sum of an integer is an integer $3(9\ell^3 - xy(3\ell)) = 3k$ for some $k \in \mathbb{Z}$. Thus by by contrapositive, if $3 \mid (x + y)$ then $3 \mid (x^3 + y^3)$.

   Hence by the two cases, if $3 \nmid (x^3 + y^3)$ if and only if $3 \nmid (x + y)$.

■

7. Bézout's identity: Let $a, b \in \mathbb{Z}$ such that a and b are not both zero. Then there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

   For example, for $a = 5$ and $b = 7$, we see $\gcd(a, b) = 1$ and we can take $x = 10$ and $y = -7$.

   Now, let $a, b, k \in \mathbb{Z}$ and assume that a, b are not both zero. Then, using Bézout's identity, show that if $k \nmid \gcd(a, b)$, then $k \nmid a$ or $k \nmid b$.

   Proof by Contrapositive:

   Let $a, b, k \in \mathbb{Z}$ and assume that a, b are not both zero. If $k \mid a$ and $k \mid b$ then $k \mid \gcd(a, b)$.

Bézout's identity: Let $a, b \in \mathbb{Z}$ such that a and b are not both zero. Then there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

Assume that $a, b \in \mathbb{Z}$ and assume that a, b are not both zero. Assume that $k \mid a$ and $k \mid b$, such that $a = kc$ and $b = kd$ for some $c, d \in \mathbb{Z}$. By Bézout's identity, we know that there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. So $\gcd(a, b) = (kc)x + (kd)y = k(cx + dy)$. Since $c, d, x, y \in \mathbb{Z}$, then $cx + dy = \ell$ for some $\ell \in \mathbb{Z}$, thus, $k \mid \ell$. Hence, $k \mid \gcd(a, b)$.

■