Assignment 1 - Thomas Boyko - 30191728

1. For each of the following statements: if the statement is true, then give a proof; if the statement is false, then write out the negation and prove that.

   (a) There exists an integer n, so that $n^3 - n$ is odd.
   The statement is false. The negation is: "For all integers n, $n^3 - n$ is even."

   Proof: Let $n \in \mathbb{Z}$.
   First we will consider the case when n is even.
   So, $n = 2k$ for some $k \in \mathbb{Z}$.
   $n^3 - n = (2k)^3 - 2k = 8k^3 - 2k = 2(4k^3 - k)$ where $(4k^3 - k) \in \mathbb{Z}$.
   So, when n is even, $n^3 - n$ is always even.

   Next is the case n is odd.
   So, $n = 2l + 1$ for some $l \in \mathbb{Z}$.
   $n^3 - n = 8l^3 + 12l^2 + 4l = 2(4l^3 + 6l^2 + 2l)$ where $(4l^3 + 6l^2 + 2l) \in \mathbb{Z}$
   So, when n is odd, $n^3 - n$ is always even.

   Since integers can only be even or odd, $n^3 - n$ is odd for any integer n. ■

   (b) $\sqrt{6}$ is irrational.

   We will prove $\sqrt{6} \notin \mathbb{Q}$ by contradiction.

   Proof: Suppose $\sqrt{6} \in \mathbb{Q}$.
   So, $\sqrt{6} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and a, b have no common factors.
   It follows that $6 = \frac{a^2}{b^2}$
   Therefore, $6b^2 = a^2$.
   We can show that $b^2 | a^2 \implies b|a$
   So a and b share a factor of b, but a and b have no common factors. (A contradiction!)
   So $\sqrt{6} \notin \mathbb{Q}$. ■

   (c) For all a, b $\in \mathbb{Z}$, if $a > 1$ and $b > 1$, then gcd(2a, 2b) = 2 gcd(a, b).

   Proof: Suppose $a, b \in \mathbb{Z}$, $a > 1, b > 1$.
   Let $c = \gcd(2a, 2b)$ where $c \in \mathbb{Z}$.
   From Bezout's identity, we know that $c = 2ax + 2by$ for some $x, y \in \mathbb{Z}$.
   So, $c = 2(ax + by)$.
   Since $c = \gcd(2a, 2b)$ and $ax + by = \gcd(a, b)$,
   $\gcd(2a, 2b) = 2\gcd(a, b)$. ■

2. Let Z + be the set of all positive integers.

   (a) Use the Euclidean Algorithm to compute $\gcd(2023, 271)$ and use that to find integers x and y so that $\gcd(2023, 271) = 2023x + 271y$.

   First we find the gcd using the Euclidean Algorithm:

$$\begin{aligned}
2023 &= 271 \times 7 + 126 \\
271 &= 126 \times 2 + 19 \\
126 &= 19 \times 6 + 12 \\
19 &= 12 \times 1 + 7 \\
12 &= 7 \times 1 + 5 \\
7 &= 5 \times 1 + 2 \\
5 &= 2 \times 2 + 1 \\
2 &= 1 \times 2 + 0
\end{aligned}$$

   So, $gcd(2023, 271) = 1$
   Next, we use the extended algorithm to find x, y.

2023	1	0
271	0	1
126	1	−7
19	−2	15
12	13	−97
7	−15	112
5	28	−209
2	−43	321
1	114	−851

   So, $\gcd(2023, 271) = 1 = 114 \times 2023 + -851 \times 271$.

(b) Find integers n, m so that $\gcd(2023, 271) = 2023m + 271n$, but $n \neq x$ and $m \neq y$. Note that x and y are the integers that you found in part (a).

Consider x, y found in part (a). If we add x to n, and subtract y from n, we are able to find another linear combination that equals $\gcd(2023, 271)$. $-385(2023) + -2874(271) = 1$.
So, $m = 385, n = -2874$.

(c) Is it true that: For all $a, b \in \mathbb{Z}^+$, if $a > 1$ and $b > 1$, then $\gcd(a, b) < \gcd(a^3, b^3)$?
Prove your answer.

The statement is false.
The negation is as follows: "$\exists a, b \in \mathbb{Z}^+$ so that $a > 1$ and $b > 1$ but $\gcd(a^3, b^3) \leq \gcd(a, b)$.

Proof: Let $a, b \in \mathbb{Z}$
Choose $a = 2$, $b = 3$.
$a^3 = 8$, $b^3 = 27$.
So, $\gcd(a, b) = \gcd(2, 3) = 1$,
And $\gcd(a^3, b^3) = \gcd(8, 27) = 1$.
So, $\gcd(a, b) = \gcd(a^3, b^3)$
Therefore, There exists $a, b \in \mathbb{Z}^+$ so that $a > 1$ and $b > 1$ but $\gcd(a^3, b^3) \leq \gcd(a, b)$. ■

3. Let P be the statement: "For all a, b, c $\in \mathbb{Z}^+$, if $\gcd(a, b) = 1$ and c divides a + b, then gcd(a, c) = 1 and gcd(b, c) = 1."

(a) Is P true? Prove your answer.

Proof: Suppose $a, b, c \in \mathbb{Z}$
Further suppose $c|a + b, \gcd(a, b) = 1$.
Let $d = \gcd(a, c)$ where d is a positive integer (according to the definition of gcd).
We now know that d divides a, c, and $a + b$.
Since d divides a and $a + b$, d must divide b.
By the definition of the greatest common denominator, d dividing a and b implies that $d \leq \gcd(a, b) = 1$.
Since $1 \leq d \leq 1$:
$d = \gcd(a, c) = 1$.
Since the order of a, b is irrelevant, this also proves that $\gcd(b, c) = 1$.
So, if $\gcd(a, b) = 1$ and $c|a + b$, then $\gcd(a, c) = 1 = \gcd(b, c)$. ■

(b) Write out the converse of P. Is the converse of P true? Prove your answer.

The converse of P is: "For all $a, b, c \in \mathbb{Z}$, if $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$, then $c|a + b$ and $\gcd(a, b) = 1$.

Proof: The statement is false. The negation is as follows:
"There exists $a, b, c \in \mathbb{Z}$ so that $\gcd(a, c) = \gcd(b, c) = 1$ but $c \nmid a+b$ or $\gcd(a, b) \neq 1$." Suppose $a, b, c \in \mathbb{Z}$.
Choose $a = 2, b = 4, c = 5$.
Note that $\gcd(2, 5) = \gcd(4, 5) = 1$.
Also note that $5 \nmid 4 + 2$.
So, the converse of P is false. ■

(c) Write out the contrapositive of P. Is the contrapositive of P true? Explain.

The contrapositive of P is: "For all $a, b, c \in \mathbb{Z}, if$ $\gcd(a, c) \neq 1$ or $\gcd(b, c) \neq 1$, then $a \nmid b + c$ or $\gcd(a, b) \neq 1$.
The contrapositive of P is true, since it is logically equivalent to P, and P is true.

(d) Write out the negation of P. Is the negation of P true? Explain.

The negation of P is: "There exists $a, b, c \in \mathbb{Z}$ so that $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$ but c does not divide $a + b$ or $\gcd(a, b) \neq 1$.
The negation of P is false, since it is logically opposite from P, and P is true.