MATH 271 ASSIGNMENT 1 SOLUTIONS

1. For each true statement below, give a proof. For each false statement below, write out its negation, then give a proof of the negation.

   (a) $\forall a, b \in \mathbb{Z}^+$, if $a|b$ and $(a+1)|b$ then $(a+2)|b$.

   (b) $\forall a, b \in \mathbb{Z}^+$, if $a|b$ and $a|(b+1)$ then $a|(b+2)$.

   (c) $\exists a \in \mathbb{Z}^+$ such that $\forall b \in \mathbb{Z}^+$, $a|b$ and $(a+1)|b$.

   (d) $\forall a \in \mathbb{Z}^+\ \exists b \in \mathbb{Z}^+$ such that $a|b$ and $(a+1)|b$.

   (e) $\forall a \in \mathbb{Z}^+\ \exists b \in \mathbb{Z}^+$ such that $a < b$, $a|b$ and $(a+1)|(b+1)$.

   (a) This statement is **false**. The negation is

   $$\exists a, b \in \mathbb{Z}^+ \text{ such that } a|b \text{ and } (a+1)|b \text{ but } (a+2) \nmid b.$$

   An example (or a counterexample to the original statement) is $a = 1$ and $b = 2$. Then $a|b$ since $1|2$, and $(a+1)|b$ since $2|2$, but $(a+2) \nmid b$ since $3 \nmid 2$.

   (b) This statement is **true**. Here is a proof.

   Let $a, b \in \mathbb{Z}^+$ be arbitrary so that $a|b$ and $a|(b+1)$. This means that $b = ak$ and $b+1 = a\ell$ for some $k, \ell \in \mathbb{Z}$. Thus $ak + 1 = a\ell$, so

   $$a(\ell - k) = a\ell - ak = 1.$$

   Since $\ell - k$ is an integer, this says that $a|1$ and so a must be equal to 1 (since $a > 0$). But then it is clear that $a|(b+2)$. This is what we wanted to prove.

   (c) This statement is **false**. The negation is

   $$\forall a \in \mathbb{Z}^+\ \exists b \in \mathbb{Z}^+ \text{ such that } a \nmid b \text{ or } (a+1) \nmid b.$$

   Here is a proof of the negation. Let $a \in \mathbb{Z}^+$ be arbitrary. We choose $b = 1$ (regardless of the value of a). Since $a + 1 \geq 2$, $(a+1) \nmid b$. Thus the negation is true, and so the original statement is false..

   (d) This statement is **true**. Here is a proof.

   Let $a \in \mathbb{Z}^+$ be arbitrary. Choose $b = a(a+1)$, which is a positive integer. Then $a|b$ (since $a + 1 \in \mathbb{Z}$) and $(a+1)|b$ (since $a \in \mathbb{Z}$).

   (e) This statement is **true**. Here is a proof.

   Let $a \in \mathbb{Z}^+$ be arbitrary. Choose $b = a(a+2)$, which is a positive integer. Then $a|b$ (since $a+2 \in \mathbb{Z}$) and $(a+1)|(b+1)$ (since $b+1 = a^2+2a+1 = (a+1)^2$ and $a+1 \in \mathbb{Z}$).

   But the question is: how could we guess that $b = a(a+2)$? One way is:

   1) get data and look for a pattern.

   - When $a = 1$, we want $1|b$ and $2|(b+1)$, and the smallest integer $b > 1$ that works is $b = 3$.
   - When $a = 2$, we want $2|b$ and $3|(b+1)$, and the smallest integer $b > 2$ that works is $b = 8$.

- When $a = 3$, we want $3|b$ and $4|(b+1)$, and the smallest integer $b > 3$ that works is $b = 15$.

And so on. Eventually (using more data if you need it) you will see that $3 = 2^2 - 1$, $8 = 3^2 - 1$, and $15 = 4^2 - 1$ (or maybe $3 = 1 \cdot 3$, $8 = 2 \cdot 4$, and $15 = 3 \cdot 5$), so it looks like b should be $(a+1)^2 - 1 = a(a+2)$. Or you might:

2) do some algebra to find b. We want $a|b$ and $(a+1)|(b+1)$, which says we want integers k and ℓ so that $b = ak$ and $b + 1 = (a+1)\ell$. Thus $ak + 1 = (a+1)\ell$, and so

$$\ell = \frac{ak+1}{a+1} = k - \frac{k-1}{a+1}\ .$$

Since ℓ and k are both integers, $\frac{k-1}{a+1}$ must be an integer too, so let's try $k - 1 = a + 1$ which says $k = a + 2$. This would mean $b = a(a+2)$.

2. (a) Prove or disprove the following statement: $\forall a \in \mathbb{R}$, if $\lfloor a \rfloor = 2$ then $\lfloor 2a \rfloor = 4$.
   (b) Write out the contrapositive of the statement in part (a). Is it true or false? Explain.
   (c) Write out the converse of the statement in part (a). Is it true or false? Explain.
   (d) Prove or disprove the following statement: $\forall r \in \mathbb{R}^+\ \exists n \in \mathbb{Z}^+$ so that $\lfloor rn \rfloor$ is prime.
   (e) Prove or disprove the following statement: $\exists n \in \mathbb{Z}^+$ so that $\forall r \in \mathbb{R}^+$, $\lfloor rn \rfloor$ is prime.

(a) This statement is **false**. A counterexample is $a = 2.5$. Then $\lfloor a \rfloor = 2$ but $\lfloor 2a \rfloor = \lfloor 5 \rfloor = 5 \neq 4$.

(b) The contrapositive is: $\forall a \in \mathbb{R}$, if $\lfloor 2a \rfloor \neq 4$ then $\lfloor a \rfloor \neq 2$. The contrapositive is false because it is logically equivalent to the original statement which is false.

(c) The converse is: $\forall a \in \mathbb{R}$, if $\lfloor 2a \rfloor = 4$ then $\lfloor a \rfloor = 2$. The converse is **true**. Here is a proof.

Let $a \in \mathbb{R}$ be arbitrary so that $\lfloor 2a \rfloor = 4$. This means that $4 \leq 2a < 5$. Therefore, dividing by 2 we get that $2 \leq a < 2.5$. So certainly $2 \leq a < 3$ which means that $\lfloor a \rfloor = 2$ which is what we want to prove.

(d) This statement is **false**. To show this we will prove that the negation is true. The negation is

$$\exists r \in \mathbb{R}^+ \text{ so that } \forall n \in \mathbb{Z}^+,\ \lfloor rn \rfloor \text{ is not prime.}$$

An example is $r = 4$. Then for any $n \in \mathbb{Z}^+$, $rn = 4n$ is an integer so $\lfloor rn \rfloor = 4n = 2 \cdot 2n$ which is not prime.

Bonus problem. Try to answer part (d) when "prime" is replaced by "composite". If you think you have an idea, talk to your professor or TA.

(e) This statement is **false**. To show this we will again prove that the negation is true. The negation is

$$\forall n \in \mathbb{Z}^+\ \exists r \in \mathbb{R}^+ \text{ so that } \lfloor rn \rfloor \text{ is not prime.}$$

Let $n \in \mathbb{Z}^+$ be arbitrary. We choose $r = 4$ (regardless of what n is). Then $\lfloor rn \rfloor = 4n = 2 \cdot 2n$ which is not prime.

Another solution would be to choose $r = 1/n$. Then $\lfloor rn \rfloor = 1$ which is not prime.

3. Let N be your student ID number.

   (a) **Use the Euclidean Algorithm** to find $\gcd(N, 271)$.

   (b) Use your answer to part (a) to write $\gcd(N, 271)$ in the form $Na + 271b$ where $a, b \in \mathbb{Z}$.

   (c) [In this part you may use results from §3.1 such as Theorem 3.1.1 on page 133 or exercises 25, 26, 27, 39, 40 or 42 from page 140. If you use any of these results, be sure to say which ones.] Let's consider all the Math 271 students' answers to part (b). Prove that no student could have correctly given integers a and b which are both even.

(a) Let's do it for the hypothetical student number $N = 123456$. The Euclidean algorithm gives:

$$\begin{aligned}
123456 &= 455 \cdot 271 + 151 & \quad (\text{so } 151 = 123456 - 455 \cdot 271)\\
271 &= 1 \cdot 151 + 120 & (\text{so } 120 = 271 - 151)\\
151 &= 1 \cdot 120 + 31 & (\text{so } 31 = 151 - 120)\\
120 &= 3 \cdot 31 + 27 & (\text{so } 27 = 120 - 3 \cdot 31)\\
31 &= 1 \cdot 27 + 4 & (\text{so } 4 = 31 - 27)\\
27 &= 6 \cdot 4 + 3 & (\text{so } 3 = 27 - 6 \cdot 4)\\
4 &= 1 \cdot 3 + 1 & (\text{so } 1 = 4 - 3)\\
3 &= 3 \cdot 1,
\end{aligned}$$

so $\gcd(123456, 271) = \mathbf{1}$, the last nonzero remainder.

(b) Now, starting with the second-last equation above, solving it for the gcd 1, and plugging in the remainders one by one from the earlier equations, we get:

$$\begin{aligned}
1 &= 4 - 3\\
&= 4 - (27 - 6 \cdot 4) = 7 \cdot 4 - 27\\
&= 7 \cdot (31 - 27) - 27 = 7 \cdot 31 - 8 \cdot 27\\
&= 7 \cdot 31 - 8 \cdot (120 - 3 \cdot 31) = 7 \cdot 31 - 8 \cdot 120 + 24 \cdot 31 = 31 \cdot 31 - 8 \cdot 120\\
&= 31 \cdot (151 - 120) - 8 \cdot 120 = 31 \cdot 151 - 39 \cdot 120\\
&= 31 \cdot 151 - 39 \cdot (271 - 151) = 70 \cdot 151 - 39 \cdot 271\\
&= 70 \cdot (123456 - 455 \cdot 271) - 39 \cdot 271 = 70 \cdot 123456 - 31850 \cdot 271 - 39 \cdot 271\\
&\qquad = 70 \cdot 123456 - 31889 \cdot 271.
\end{aligned}$$

So $a = 70$ and $b = -31889$ in this case.

(c) We'll prove this by contradiction. Suppose that some student (with student ID N) found a correct answer where both a and b were even. Suppose that $\gcd(N, 271) = d$. So the student would have obtained the equation $Na + 271b = d$, so d must be even since both a and b are even. (This uses Theorem 3.1.1 on page 133 and exercise 42 (twice) on page 140.) But since 271 is odd and $d|271$ this means that d must be odd. (In fact, 271 is prime which means that d can only be 1 or 271, but we don't need to know that.) This is a contradiction, so a and b cannot both be even.