EXAM 1

MATH 311W, SPRING 2016

Be sure to show all your work for full points. Answers without accompanying work will not be given full credit. The exam is worth a total of 100 pts. Please write your name below.

Solutions
1). (10 pts) Show that any natural number $n \geq 2$ is a product of prime numbers.

**First solution:** We argue by strong induction. The base case $n = 2$ is clear, since 2 is a prime. Now suppose that any number $k \in \{2, 3, \ldots, n - 1\}$ is a product of primes. We have to show that $n$ is as well. There are two cases. If $n$ is prime, we are done. Otherwise, $n$ is composite, so we can write $n = ab$ with $a, b \in \{2, 3, \ldots, n - 1\}$. By the induction hypothesis, there are primes $p_j, q_j$ such that

$$a = p_1 p_2 \ldots p_r, \quad b = q_1 q_2 \ldots q_s,$$

in which case

$$n = p_1 p_2 \ldots p_r q_1 q_2 \ldots q_s$$

is a product of primes.

**Second solution:** As induction is equivalent to the well-ordering principle, it is not surprising that there is a proof using this principle as well, which several have discovered on the exam either formally or intuitively. Note that when thinking about this problem for specific numbers, one might think of the following algorithm. If $n$ is not prime, it factors as a product of smaller numbers. Look at these two smaller numbers and see whether they are prime, and continue until you are left only with primes. In what follows, I give a formal proof which this reasoning underlies.

Let $X$ be the set of natural numbers which are $\geq 2$ and do not factor as a product of primes. Suppose, for the sake of contradiction, that $X \neq \emptyset$. Then by the Well-Ordering Principle, $X$ has a smallest element, say $k$. As $k$ isn’t a product of primes, in particular it isn’t prime, and so we can write $k = ab$ with $2 < a, b < k$. By the minimality assumption on $k$, $a, b \not\in X$, which means that $a, b$ are products of primes. But this is a contradiction, as then $k = ab$ is a product of the primes among the factorizations of $a, b$, and so is a product of primes, and hence doesn’t lie in $X$. 
2). (15 pts) Construct a truth table for \((p \rightarrow q) \lor (q \rightarrow p)\). Use the table to decide whether this is a tautology, contradiction, or neither.

Here is the truth table:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>(p \rightarrow q)</th>
<th>(q \rightarrow p)</th>
<th>((p \rightarrow q) \lor (q \rightarrow p))</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

As the last column consists only of \(T\)'s, this is a tautology. In words, the reason this statement is a tautology is that if either \(p\) or \(q\) is false, then by definition one of the two implications is automatically true, and if neither is false, then clearly both implications hold.
3). (15 pts) Use the Euclidean algorithm to find $\gcd(51, 36)$. Factor 51 and 36 as products of primes. Use these factorizations to find $\text{lcm}(51, 36)$ (you don’t have to multiply all the terms out). Express $\gcd(51, 36)$ in the form $51r + 36s$ with $r, s \in \mathbb{Z}$.

To find $\gcd(51, 36)$, we compute

\[
\begin{align*}
51 &= 1 \cdot 36 + 15 \\
36 &= 2 \cdot 15 + 6 \\
15 &= 2 \cdot 6 + 3 \\
6 &= 2 \cdot 3 + 0,
\end{align*}
\]

so the gcd is 3. We can factor into primes as

\[
\begin{align*}
51 &= 2^0 \cdot 3^1 \cdot 17^1 \\
36 &= 2^2 \cdot 3^2 \cdot 17^0,
\end{align*}
\]

which shows that

\[
\text{lcm}(51, 36) = 2^{\max(0, 2)} \cdot 3^{\max(1, 2)} \cdot 17^{\max(1, 0)} = 2^2 \cdot 3^2 \cdot 17^1.
\]

We can also find an integral linear combination of 51 and 36 equal to the gcd 3 as follows, using the equations from the Euclidean algorithm above:

\[
3 = 15 – 6 \cdot 2 = 15 – (36 – 15 \cdot 2) \cdot 2 = 15 \cdot (5) + 36 \cdot (-2) = (51 – 36) \cdot (5) + 36 \cdot (-2) = 51 \cdot (5) + 36 \cdot (-7).
\]
4). (15 pts) Show that if $a, b, c \in \mathbb{N}$ are chosen with $a$ and $b$ relatively prime, and $a|bc$, then $a|c$.

The trick is to use the fact that if $(a, b) = 1$, then there are integers $r, s$ such that

$$ar + bs = 1.$$ 

Multiplying this equation by $c$, we get

$$car + cbs = c.$$ 

Now $a|car$, and if $a|bc$, then $a|cbs$ so that $a$ divides $car + cbs = c$, as desired.
5). (15 pts) Show that $11^n - 6$ is divisible by 5 for every positive integer $n$.

**First solution:**
We argue by induction. In the base case, when $n = 1$, $11^1 - 6 = 5$ is divisible by 5. Now suppose that $11^n - 6$ is divisible by 5. We must show that $11^{n+1} - 6$ is also divisible by 5. Indeed, we compute that

$$11^{n+1} - 6 = 11 \cdot 11^n - 6 = (10 + 1) \cdot 11^n - 6 = 10 \cdot 11^n + (11^n - 6).$$

By the induction hypothesis, $5 | (11^n - 6)$, and of course $5 | 10 \cdot 11^n$, which establishes the claim.

**Second solution:**
Alternatively, using the modular arithmetic we are learning now, one can compute that $11^n - 6 \equiv 1^n + 4 \equiv 5 \equiv 0 \pmod{5}$. A few people also intuitively noticed the connection to the following observation. Note that if you multiply a bunch of 11’s together, if you think about how the multiplication works (write down a few first cases!), then you will always have a number ending in 1. In other words, $11^n \equiv 1^n \equiv 1 \pmod{10}$. Thus, in fact $11^n - 6 \equiv -5 \equiv 5 \pmod{10}$, which is in fact a stronger statement.
6). (15 pts) Suppose that $R$ is an equivalence relation on $X$. Show that the sets $[x]_R = \{y \in X : yRx\}$ as $x$ ranges over elements of $X$ form a partition of $X$.

We first show that if $b \in [a]_R$ (i.e., that $bRa$), then $[a]_R = [b]_R$. We do this by showing that both sets contain the other. Now, if $c \in [b]_R$, then by definition $cRb$, and we said before that $bRa$, so by transitivity of $R$, we have $cRa$, which shows that $c \in [a]_R$. Hence, $[b]_R \subseteq [a]_R$. In the other direction, suppose that $c \in [a]_R$, or $cRa$. Then by symmetry of $R$ we have $aRb$, so transitivity then implies that $cRb$. Hence, $c \in [b]_R$, and we have shown $[a]_R \subseteq [b]_R$ as well.

Now, by the reflexive property of $R$, we have that $x \in [x]_R$ for all $x \in X$, and so the sets $[x]_R$ cover $X$. To show they are disjoint, suppose that $[x]_R \cap [y]_R \neq \emptyset$, and say $z \in [x]_R \cap [y]_R$. Then by the property we showed in the last paragraph, $z \in [x]_R$ implies that $[z]_R = [x]_R$, and similarly $z \in [y]_R$ implies that we also have $[z]_R = [y]_R$, and so $[x]_R = [y]_R$. 
7). (15 pts) Show that a function \( f: X \to Y \) has an inverse if and only if it is a bijection.

We first show that an invertible function \( f \) is always a bijection. To show injectivity, suppose that \( f(x) = f(x') \). Then applying \( f^{-1} \) to both sides shows that \( x = x' \). To show surjectivity, suppose that \( y \in Y \). A preimage for \( y \) under \( f \) is given by \( f^{-1}(y) \in X \), since \( f(f^{-1}(y)) = y \).

Now suppose that \( f \) is a bijection. We can see that \( f \) is invertible by constructing its inverse. As \( f \) is a bijection, for each \( y \in Y \), surjectivity shows that there is at least one \( x \in X \) such that \( f(x) = y \), and injectivity shows that there is at most one such \( x \). That is, each \( y \in Y \) is mapped to under \( f \) by a unique \( x \in X \). Thus, the map \( g: Y \to X \) given by sending each \( y \) to the \( x \) for which \( f(x) = y \) is a well-defined function. We claim that \( g \) is an inverse for \( f \). To see this, we must consider both compositions and check that we obtain the identity functions. Using the notation above, for all \( x \in X \), \( y \in Y \), we have

\[
\begin{align*}
gf(x) &= g(y) = x, \\
gf(y) &= f(x) = y,
\end{align*}
\]

so that \( gf = \text{id}_X \) and \( fg = \text{id}_Y \). That is, \( g = f^{-1} \).