1. Counting with sets

(a) In our role-playing game, an evil character may be an elf or a troll, it may be red, green, brown, or black, and it may have scales or hair. A good character may be an elf or a human or a lion, it may be green, brown, or blue, and it has hair or fur. How many different character types do we have?

Solution: There are $2 \cdot 4 \cdot 2 = 16$ types of evil characters. There are $3 \cdot 3 \cdot 2 = 18$ types of good characters. But there are 2 types of characters that could be good or evil. So we have a total of $16 + 18 - 2 = 32$ possible appearances.

(b) Suppose we have a 26 character alphabet. How many 6-letter strings start with PRE or end with TH?

Solution: There are $26^3$ strings starting with PRE, $26^4$ strings ending in TH, and 26 strings that start with PRE and end in TH. Thus we have a total of $26^3 + 26^4 - 26 = 26(26^2 + 26^3 - 1)$ total strings.

(c) How many different 6-letter strings can I make out of the letters in the word “illini”?

Solution: We calculate the number of permutations of 6 letters ($6!$) and divide out by the double-counting of the possibilities for l (2!) and for i (3!). This gives us $\frac{6!}{2!3!} = 5 \cdot 4 \cdot 3 = 60$ possible strings.

2. Euclidean algorithm

Trace the execution of the Euclidean algorithm for computing GCD on the inputs $a = 837$ and $b = 2015$. That is, give a table showing the values of the main variables $(x, y, r)$ for each pass through the loop. Explicitly indicate what the output value is.

Solution:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>837</td>
<td>2015</td>
<td>837</td>
</tr>
<tr>
<td>2015</td>
<td>837</td>
<td>341</td>
</tr>
<tr>
<td>837</td>
<td>341</td>
<td>155</td>
</tr>
<tr>
<td>341</td>
<td>155</td>
<td>31</td>
</tr>
<tr>
<td>155</td>
<td>31</td>
<td>0</td>
</tr>
<tr>
<td>31</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Therefore, the algorithm outputs GCD(837, 2015) = 31. Note that the algorithm terminates when y = 0, not when r = 0.
3. Direct Proof Using Congruence mod k

In the book, you will find several equivalent ways to define congruence mod k. For this problem, use the following definition: for any integers $x$ and $y$ and any positive integer $m$, $x \equiv y \pmod{m}$ if there is an integer $k$ such that $x = y + km$.

Using this definition prove that, for all integers $a$, $b$, $c$, $p$, $q$ where $p$ and $q$ are positive, if $a \equiv b \pmod{p}$ and $c \equiv b \pmod{q}$ and $q|p$, then $a - 2c \equiv (-b) \pmod{q}$.

Solution:

Let $a$, $b$, $c$, $p$, $q$ be integers, where $p$ and $q$ are positive. Suppose that $a \equiv b \pmod{p}$ and $c \equiv b \pmod{q}$ and $q|p$. By the given definition of congruence, $a = b + pr$ and $c = b + qt$, where $r$ and $t$ are integers. Since $q|p$, we know that $p = qu$, where $u$ is an integer.

Therefore, by substituting $b + pr$ for $a$ and $b + qt$ for $c$:

$$a - 2c = b + pr - 2(b + qt)$$

By substituting $qu$ for $p$, we get:

$$
\begin{align*}
    a - 2c & = b + qu r - 2(b + qt) \\
            & = b + qu r - 2b - 2qt \\
            & = (-b) + q(ur - 2t) \\
            & = (-b) + qw
\end{align*}
$$

where $w = ur - 2t$. By closure, $w$ must be an integer. Therefore, by the definition given for congruence, $a - 2c \equiv (-b) \pmod{q}$. 

4. Equivalence classes

Let \( A = \mathbb{R}^{\geq 0} \times \mathbb{R}^{\geq 0} - \{(0, 0)\} \), i.e. pairs of non-negative reals in which no more than one of the two numbers is zero.

Consider the equivalence relation \( \sim \) on \( A \) defined by

\[
(x, y) \sim (p, q) \text{ iff } (xy)(p + q) = (pq)(x + y)
\]

(a) List four elements of \([3, 1]\). Hint: what equation do you get if you set \((x, y)\) to \((3, 1)\) and \(q = 2p\)?

(b) Give two other distinct equivalence classes that are not equal to \([3, 1]\).

(c) Describe the members of \([0, 4]\).

Solutions:

(a) \((3, 1), (1, 3), (\frac{9}{8}, \frac{9}{4}), (\frac{9}{4}, \frac{9}{8})\). You can find a range of other elements by setting \(q\) to other multiples of \(p\).

(b) For example, \([3, 2]\), \([3, 4]\)

(c) All pairs of the form \((0, y)\) or \((x, 0)\).

If \((x, y) = (0, 4)\), then the equation \((xy)(p + q) = (pq)(x + y)\) reduces to \(0(p + q) = (pq)4\). So this means either \(p\) or \(q\) must also be zero and, then, it doesn’t matter what value we give to the other.
5. **Functions**

For each of the following functions determine if it is onto or not onto. Briefly, but clearly, justify your answers. (A full formal proof is not required.)

(a) The function $f$ given by the following diagram where the left bubble represents the domain and the right the codomain:

![Diagram of function f](image)

**Solution:** The function $f$ is onto because every output has at least one corresponding input that the function maps to it.

(b) The function $g$ given by the following diagram:

![Diagram of function g](image)

**Solution:** The function $g$ is not onto because the codomain element $(3, 1)$ has no corresponding input that maps to it.

(c) $h : \mathbb{Z} \to \mathbb{Z}$ such that $h(x) = 3\lceil \frac{x}{3} \rceil$

**Solution:** The function $h$ is not onto because 1 is not in the image of the function. If it were, then $1 = 3\lceil \frac{x}{3} \rceil$ which is impossible because $\lceil \frac{x}{3} \rceil$ is an integer.

(d) $k : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ by $k(x, y) = x$

**Solution:** The function $k$ is onto. Pick any codomain element $x \in \mathbb{R}$. Consider $(x, 0) \in \mathbb{R} \times \mathbb{R}$. Notice that $k(x, 0) = x$, so $x$ has a pre-image.
6. **One-to-one**

Which of these functions are one-to-one? Briefly justify your answers.

(a) \( h : [0, 1] \rightarrow \mathbb{R}^2 \) such that \( h(\lambda) = \lambda(2, 2) + (1 - \lambda)(1, 3) \) where you use the following formula to multiply a real number \( a \) by a 2D point \((x, y)\):

\[
a(x, y) = (ax, ay)
\]

**Solution**

\( h \) is one-to-one. In \( \mathbb{R}^2 \), \( h \) describes the strictly increasing line segment between the points \((2,2)\) and \((1,3)\).

(b) \( f : \mathbb{N}^2 \rightarrow \mathbb{N} \) such that \( f(x, y) = 4^x 3^y \)

**Solution**

\( f \) is one-to-one. The image of \( f \) is the set of positive integers that have only 2 and 3 as prime factors and the prime factorization of any integer is unique.

(c) \( k : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z} \) such that \( k(x, y) = (1 - x^2) \left\lfloor \frac{y}{3} \right\rfloor \)

**Solution**

\( k \) is not one-to-one. \((0,0)\) and \((1,0)\) are both mapped to 0.

7. **Subset proof**

Suppose that \( A, B \) and \( C \) are sets. Recall the definition of \( X \subseteq Y \): for every \( p \), if \( p \in X \), then \( p \in Y \). Prove that if \( A \subseteq B \) then \( A \cap C \subseteq B \cap C \). Briefly justify the key steps in your proof.

**Solution:** Suppose that \( p \in A \cap C \). Then \( p \in A \) and \( p \in C \), by the definition of intersection. Since \( p \in A \) and \( A \subseteq B \), \( p \in B \) (definition of subset). So \( p \in B \) and \( p \in C \), which implies that \( p \in B \cap C \) (definition of intersection).