Math 136, Spring ’15

Project 1: The Stamp Problem
first draft due Wednesday, Feb 11
final version due Wednesday, Feb 25

Given positive integers $a$ and $b$, this project looks at the question of what integers can and cannot be represented by $ma + nb$ where $m$ and $n$ are non-negative integers (integers greater than or equal to 0). It is sometimes referred to as the stamp problem because you can think of it as asking what postage amounts can you make if you are restricted to an unlimited supply of $a\frac{c}{c}$ stamps and $b\frac{c}{c}$ stamps.

(1) In the list given below, cross out the postage amounts that can be made using $5\frac{c}{c}$ stamps and $8\frac{c}{c}$ stamps.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
</tr>
<tr>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
</tr>
<tr>
<td>30</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
</tr>
<tr>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
</tr>
</tbody>
</table>

(2) What are the amounts that cannot be made? How do you know that there are no larger amounts that cannot be made?

(3) If you start with $4\frac{c}{c}$ stamps and $9\frac{c}{c}$ stamps, what are the postage amounts that cannot be made? What if you had started with $4\frac{c}{c}$ stamps and $6\frac{c}{c}$ stamps?

(4) When you have two kinds of stamps, when will there be a largest postage amount that you cannot make?

(5) If you start with $a\frac{c}{c}$ stamps and $b\frac{c}{c}$ stamps, what is the largest postage amount that you cannot make?

Continued on other side.
(6) Justify your answer to the previous question. It is helpful to use the language of modular arithmetic. Notice that for 5¢ stamps and 8¢ stamps, when you put the different amounts into different columns, you were really arranging the amounts so that all of those in the same column were congruent modulo 5. For a given modulus m and an integer r, 0 ≤ r < m, we call the set of integers that are congruent to r modulo m, the equivalence class of r modulo m. Each column consists of the non-negative integers in one of the equivalence classes modulo 5.

Assume that a and b are relatively prime, and consider the first a non-negative multiples of b: 0 \cdot b, 1 \cdot b, \ldots, (a - 1) \cdot b.

(a) Prove that no two of them can be in the same column, and therefore every column contains exactly one of these multiples of b. Be certain to use your assumption that a and b are relatively prime.

(b) Explain why the smallest amount that can be made in any column must be a multiple of b.

(c) Explain why there must be a column (equivalence class) for which the smallest amount that can be made is (a - 1)b. Once you have proven these statements, then use them to complete the proof of your formula.

(7) If a and b are relatively prime, how many positive integers cannot be represented by ma + nb where m and n are non-negative integers? Find a formula in terms of a and b and then prove that it is correct. Hint:

(a) The floor of a rational number, x/y, is defined to be the largest integer less than or equal to x/y. It is written as \lfloor x/y \rfloor. For example, \lfloor 12/5 \rfloor = 2. Explain why the number of amounts that cannot be made is

\left\lfloor \frac{b}{a} \right\rfloor + \left\lfloor \frac{2b}{a} \right\rfloor + \cdots + \left\lfloor \frac{(a - 1)b}{a} \right\rfloor.

(b) Prove that the sum that you found in part (a) is equal to

\frac{b}{a} + \frac{2b}{a} + \cdots + \frac{(a - 1)b}{a} - \frac{1}{a} - \frac{2}{a} - \cdots - \frac{a - 1}{a}.

(c) Find and prove the formula for the sum of the first a - 1 positive integers, 1 + 2 + \cdots + (a - 1), and combine it with the result proved in part (b) to find a closed formula for the desired number of integers.
Working groups are made of three or four students. Each working group of four students is split into two writing teams. Students who are responsible for writing up the project report together are connected by an & (ampersand). If a writing team is not working, please let the other member(s) of the team and me know. I will allow the team to break up and each member to submit their own report.
Writing up your report. This must be written up as a report, not a sequence of answers. You need a title and an introduction that explains to the reader what this report will reveal and why it is worth the reader’s time to read it. When you write out the report, you may not assume that your reader has seen any of the questions or knows anything about modular arithmetic. Explain what you did and why you did it, and clearly prove each of the assertions that you make. The report must end with a conclusion that summarizes the important points of the report.

Note the four aspects of the writing rubric that I will be looking for as I grade this paper:

Framing. Does the paper provide a clear statement of the main result? Does the introduction to the paper clearly identify why this result matters and what is at stake?

Development of Argument. Are the mathematical arguments correct and complete? Are the logical arguments clear to the reader?

Writing Quality. Does the paper proceed in a progressive, logical order? Are the paragraphs coherent and unified? Does the paper demonstrate appropriate sentence construction and word choice, including correct use of mathematical and other technical terminology?

Global Qualities. Does the paper show few errors in punctuation, spelling, and formatting? Overall, was the paper enjoyable? How did it perform in relation to expectations?
Appendix: The Language of Modular Arithmetic

It is useful to have a way of referring to all of the numbers in a given column by specifying any one of the numbers in that column. When we refer to “3 modulo 5,” we mean any of the numbers in the column that includes 3 when we separate the integers into 5 columns. For this reason, “3 modulo 5” is the same as 8 or 13 or 128 modulo 5, and we write

\[ 3 \equiv 8 \pmod{5}, \]

read “3 is congruent to 8 modulo 5,” to mean that 3 and 8 are in the same column out of 5.

The numbers in any one column are those that have the same remainder when divided by 5: 3, 8, 13, and 128 each leave a remainder of 3 when divided by 5. Two integers are congruent modulo \( m \) if they leave the same remainder when divided by \( m \).

Another way of thinking of this is that 5 divides the difference between any two numbers in the same column. This makes it easier to extend the definition to negative numbers: \(-2 \equiv 3 \pmod{5}\). Two integers are congruent modulo \( m \) if and only if their difference is a multiple of \( m \):

\[ a \equiv b \pmod{m} \iff m \text{ divides } b - a. \] (1)

Each column constitutes an equivalence class, also often called a residue class, which means that we treat all of its members as equivalent. There are three properties that an equivalence must satisfy. Use the definition of congruence in terms of divisibility as given in equation (1) to show that each of these properties is satisfied for modular congruence.

(1) Each element is equivalent to itself. Why is it true that \( a \equiv a \pmod{m} \)?

(2) If \( a \) is equivalent to \( b \), then \( b \) must be equivalent to \( a \). Why is it true that \( a \equiv b \pmod{m} \) implies \( b \equiv a \pmod{m} \)?

(3) Equivalence must be transitive. This means that if \( a \) is equivalent to \( b \) and \( b \) is equivalent to \( c \), then \( a \) must be equivalent to \( c \). Why is it true that \( a \equiv b \pmod{m} \) and \( b \equiv c \pmod{m} \) implies \( a \equiv c \pmod{m} \)?

The number of columns is called the modulus. Arithmetic on these equivalence classes is called modular arithmetic. The word modulo is a preposition. (How often do you get to learn a new preposition?) The modulus is its object. The phrase “3 modulo 5” is shorthand for “the equivalence class containing 3 for the modulus 5.”