**Class Work: Modular Arithmetic**
This is a full-time activity worth 10 points.

## Problem of the Day

Choose ONE of the following to do:

1. This problem is for those who want to work with divisibility tests, like the one for divisibility by 3 explored in Screencast 7.4.3.

   (a) The divisibility test for 3 and for 9 say the same basic thing: If an integer's digit sum is divisible by 3 (or 9), then the integer itself is divisible by 3 (or 9). Does this trick work for 11? That is, if an integer's digit sum is divisible by 11, does it follow that the integer itself is divisible by 11?

   (b) Here's a test for divisibility by 11:

   > If an integer is such that the difference between the sum of the odd-numbered digits (first, third, fifth, etc.) and the sum of the even-numbered digits (second, fourth, sixth, etc.) is divisible by 11, then the integer itself is divisible by 11.

   Check that this test works (using both an example and a non-example) and then prove that it works in the case of a five-digit integer. Hint: As in the proof of divisibility by 3, let $n$ be the integer in question and start by writing

   $$n = \cancel{d_5 \times 10^5 +} d_4 \times 10^4 + d_3 \times 10^3 + d_2 \times 10^2 + d_1 \times 10^1 + d_0$$

   Here are some questions to answer before you prove this:

   - What are the odd digits and the even digits here? And, does it matter which group of digits is which in the context of the divisibility test?
   - What does it mean to say that "the difference between the sum of the odd-numbered digits and the sum of the even-numbered digits is divisible by 11" in terms of $d_0, d_1, \ldots, d_5$?
   - What are the equivalence classes of $1, 10, 100, 1000$, and $10000$ mod 11?
   - Why is $[10] = [-1]$ mod 11?

2. This problem is for those who want to work with the *affine cipher* described and instantiated in Screencast 7.4.4[1]. Let $m = 10$ and $b = 5$.

   (a) Encrypt the message `ATTACK` using the affine cipher and the values of $m$ and $b$ above. The ciphertext (encrypted message) should be in the form of characters, not equivalence classes.

   (b) Find the element $[n]$ of $\mathbb{Z}_{29}$ such that $[10] \odot [n] = [1]$.

   (c) Find the element $[c]$ of $\mathbb{Z}_{29}$ such that $[c] \oplus [5] = [0]$.

   (d) Suppose you receive the message: `VRQQTG`. This was sent to you by someone using the same values of $m$ and $b$ as before. Decrypt the message.

[1] If you liked that example and have space in your schedule in Winter 2014, I will be teaching a new General Education course called **MTH 312: Cryptography and Privacy** that will go into this and many other aspects of cryptography and information security from a mathematical perspective.

(e) Suppose Eve, an evil eavesdropped, intercepts the encrypted message you created earlier. Describe how Eve could try to break the code and recover the original message without knowing the values of $m$ or $b$. Be creative!

**Extra**: In the third screencast, it mentioned that the proof of divisibility by 3 — which was restricted only to four-digit integers — could easily be extended to integers of arbitrary length by using the fact that

For all natural numbers $n$, $[10^n] = [1]$ under the relation of congruence mod 3.

Prove this fact. (Hint: Notice that it's stated "for all natural numbers". What does that suggest regarding proof strategy?)

## Parameters

If your group finishes your work, please hand it in at the end of class. If all groups finish by the end of class, we will take time to debrief the solutions to one or more of these.