Winter 2017, Math 148: Week 1 Problem Set
Due: Wednesday, January 18th, 2017
Modular Arithmetic

Discussion problems. The problems below should be completed in class.

(D1) *Modular addition and multiplication.*

(a) Determine which of the following are true without using a calculator.

(i) $1234567 \cdot 90123 \equiv 1 \bmod 10$.
(ii) $2468 \cdot 13579 \equiv -3 \bmod 25$.
(iii) $2^{58} \equiv 3^{58} \bmod 5$.
(iv) $1234567 \cdot 90123 = 111262881711$.

(b) The *order* of an element $a \in \mathbb{Z}_n$ is the smallest integer k such that adding a to itself k times yields $0 \in \mathbb{Z}_n$.

(i) Find the order of every element of $\mathbb{Z}_{12}$.
(ii) Find a formula for the order of $[x] \in \mathbb{Z}_n$ with $0 \leq x \leq n-1$ in terms of x and n. Briefly justify your formula (you are not required to write a formal proof).
(iii) For which n does every nonzero element of $\mathbb{Z}_n$ have order n?

(D2) *Divisibility rules.* In class yesterday, we saw (and proved!) a trick that let us to quickly determine when an integer is divisible by 9.

(a) Prove that an integer x is divisible by 3 if and only if the sum of its digits (in base 10) is divisible by 3.

(b) Using part (a), develop a criterion for when an integer is divisible by 15.

(D3) *Multiplicative inverses.* Two elements $a, b \in \mathbb{Z}_n$ are *multiplicative inverses* if $a \cdot b = [1]_n$. An element $a \in \mathbb{Z}_n$ is *invertible* if it has a multiplicative inverse.

(a) Determine which elements of $\mathbb{Z}_6$, $\mathbb{Z}_7$ and $\mathbb{Z}_8$ have multiplicative inverses.

(b) What do you notice about your answer to part (a)? State your conjecture formally.

(c) Prove that $[1]_n$ is invertible in $\mathbb{Z}_n$. Prove that $[0]_n$ is not invertible in $\mathbb{Z}_n$.

(D4) *Cartesian products.* Given positive integers m and n, let

$$\mathbb{Z}_n \times \mathbb{Z}_m = \{(a, b) : a \in \mathbb{Z}_n, b \in \mathbb{Z}_m\}.$$

In particular, each element of $\mathbb{Z}_n \times \mathbb{Z}_m$ is an ordered pair whose first value is an element of $\mathbb{Z}_n$ and whose second value is an element of $\mathbb{Z}_m$. Define addition and multiplication on $\mathbb{Z}_n \times \mathbb{Z}_m$ by $(a, b) + (a', b') = (a + a', b + b')$ and $(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$, respectively.

(a) How many elements does $\mathbb{Z}_n \times \mathbb{Z}_m$ have?

(b) The *order* of an element $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m$ is the smallest integer k such that adding (a, b) to itself k times yields $(0, 0)$ (or, written more compactly, $k(a, b) = (0, 0)$).

(i) What is the highest order of an element of $\mathbb{Z}_5 \times \mathbb{Z}_3$? What about $\mathbb{Z}_6 \times \mathbb{Z}_4$?
(ii) Can you give a general formula for the highest order of an element in $\mathbb{Z}_n \times \mathbb{Z}_m$?

(c) Which elements of $\mathbb{Z}_n \times \mathbb{Z}_m$ are invertible?

Required problems. As the name suggests, you must submit *all* required problem with this homework set in order to receive full credit.

(R1) Write the addition and multiplication tables for $\mathbb{Z}_6$. You can leave off the bracket notation and simply denote the elements by $0, 1, 2, 3, 4, 5 \in \mathbb{Z}_6$.

(R2) Find all simultaneous solutions to the equations

$$x + 2y = 4 \qquad \text{and} \qquad 4x + 3y = 4$$

in $\mathbb{Z}_7$. Do the same in $\mathbb{Z}_6$.

(R3) Prove that an integer x is divisible by 4 if and only if the last two digits of x in base 10 form a 2-digit number that is divisible by 4.

(R4) Prove that if x and y are each invertible in $\mathbb{Z}_n$, then xy and x^{-1} (meaning the multiplicative inverse of x) are invertible in $\mathbb{Z}_n$.

Selection problems. You are required to submit all parts of *one* selection problem with this problem set. You may submit additional selection problems if you wish, but please indicate what you want graded. Although I am happy to provide written feedback on all submitted work, no extra credit will be awarded for completing additional selection problems.

(S1) (a) Suppose $(x_n \cdots x_1 x_0)_{10}$ expresses x in base 10. Prove that

$$x \equiv x_0 - x_1 + x_2 - x_3 + \cdots + (-1)^n x_n \bmod 11.$$

(b) Use part (a) to decide whether 1213141516171819 is divisible by 11.

(S2) Determine whether each of the following is true or false. Prove each true statement, and give a counterexample for each false statement. For each, assume that $n \geq 2$ and $x, y, z \geq 0$ are all integers.

(a) If $x \equiv y \bmod n$, then $xz \equiv yz \bmod n$.

(b) If $xz \equiv yz \bmod n$, then $x \equiv y \bmod n$.

(c) If $xy \equiv 0 \bmod n$, then $x \equiv 0 \bmod n$ or $y \equiv 0 \bmod n$.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) We saw in class that an integer x is divisible by 9 if and only if the sum of the digits (base 10) of x is divisibile by 9, and you proved in discussion that the same holds for divisibility by 3. Fix a base b. State and prove a characterization of the n for which any integer x is divisible by n if and only if the sum of the digits (base b) of x is divisible by n (in particular, for $b = 10$, this only holds for $n = 3$ and $n = 9$).