Winter 2018, Math 148: Week 1 Problem Set
Due: Wednesday, January 17th, 2018
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) $1234567 \cdot 90123 = 111262881711$.
(v) There exists $x \in \mathbb{Z}$ such that $x^2 + x \equiv 1 \bmod 2$.
(vi) There exists $x \in \mathbb{Z}$ such that $x^3 + x^2 - x + 1 = 1522745$.

(b) Determine whether each of the following is true or false. Give an explanation for each true statement, and a counterexample for each false statement. Assume throughout that $n \geq 2$ and $x, y, z \geq 0$ are all integers.

(i) If $x \equiv y \bmod n$, then $xz \equiv yz \bmod n$.
(ii) If $xz \equiv yz \bmod n$, then $x \equiv y \bmod n$.
(iii) If $xy \equiv 0 \bmod n$, then $x \equiv 0 \bmod n$ or $y \equiv 0 \bmod n$.

(c) The *order* of an integer $x \in \{0, \ldots, n-1\}$ modulo n is the smallest integer k such that adding x to itself k times yields 0 modulo n, that is $kx \equiv 0 \bmod n$.

(i) Find the order of each integer $x = 0, \ldots, 11$ modulo $n = 12$.
(ii) For which n does every nonzero x have order n?
(iii) Find a formula for the order of x modulo n in terms of x and n. Briefly justify your formula (you are not required to write a formal proof).

(D2) *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 $\mathbb{Z}_n$.

(D3) *Divisibility rules.* In the last lecture, 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.

Required problems. As the name suggests, you must submit *all* required problems 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 $[\ \ ]_6$ notation and simply denote the elements by $0, 1, 2, 3, 4, 5 \in \mathbb{Z}_6$.

(R2) Determine whether each of the following statements is true or false. Justify your answer (you are not required to give a formal proof). You may *not* use a calculator.

(a) 14323341327 is prime.

(b) There exists $x \in \mathbb{Z}$ such that $x^2 + 1 = 123456789$.

(R3) Find all $x, y \in \mathbb{Z}_7$ that are solutions to both of the equations

$$x + 2y = [4]_7 \qquad \text{and} \qquad 4x + 3y = [4]_7$$

in $\mathbb{Z}_7$. Do the same for $x, y \in \mathbb{Z}_6$ (where $[4]_7$ is replaced with $[4]_6$).

(R4) 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.

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) The goal of this question is to prove that the "freshman's dream" equation

$$(x + y)^p = x^p + y^p$$

holds for any $x, y \in \mathbb{Z}_p$ when p is prime.

(a) Recall that for any $n, k \geq 0$,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

is an integer. Prove that if p is prime and $1 \leq k \leq p - 1$, then p divides $\binom{p}{k}$.

(b) Recall that for any $x, y \in \mathbb{R}$,

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Use this to prove the Freshman's Dream equation for $x, y \in \mathbb{Z}_p$.

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 the following holds: an integer x is divisible by n if and only if the sum of the digits (base b) of x is divisible by n. As an example, for $b = 10$, this only holds for $n = 3$ and $n = 9$.