Spring 2019, Math 320: Problem Set 3
Due: Tuesday, February 19th, 2019
Modular Arithmetic

Discussion problems. The problems below should be worked on in class.

(D1) *Modular addition and multiplication.* Determine which of the following are true without using a calculator.

(a) $1234567 \cdot 90123 \equiv 1 \bmod 10$.
(b) $2^{58} \equiv 3^{58} \bmod 5$.
(c) $2468 \cdot 13579 \equiv -3 \bmod 25$.
(d) $1234567 \cdot 90123 = 111262881731$.
(e) There exists $x \in \mathbb{Z}$ such that $x^2 + x \equiv 1 \bmod 2$.
(f) There exists $x \in \mathbb{Z}$ such that $x^3 + x^2 - x + 1 = 1522745$.

(D2) *Divisibility rules.* In the last lecture, we previewed a trick that let us to quickly determine when an integer is divisible by 9. In what follows, fix a positive integer a, and suppose $(a_r \cdots a_1 a_0)_{10}$ is the expression of a in base 10, with $0 \le a_i \le 9$ for each i.

(a) Complete the following proof that $a \equiv (a_r + \cdots + a_1 + a_0) \bmod 9$. Be clear which modular arithmetic property is used for each equality!

Proof. Expressing a in terms of its digits $a_0, a_1, \ldots, a_r$, we obtain

$$\begin{aligned}[a]_9 &= [a_r(\underline{\qquad}) + \cdots + a_2 10^2 + a_1 10 + a_0]_9 \\ &= \underline{\qquad\qquad\qquad} \\ &\vdots \\ &= \underline{\qquad\qquad\qquad} \\ &= [a_r + \cdots + a_1 + a_0]_9,\end{aligned}$$

meaning $a \equiv (a_r + \cdots + a_1 + a_0) \bmod 9$. □

(b) Prove that $9 \mid a$ if and only if the sum of the digits of a is divisible by 9.
(c) Modify your proof in part (a) to prove that an integer a is divisible by 3 if and only if the sum of its digits (in base 10) is divisible by 3.
(d) Using part (c), develop a criterion for when an integer is divisible by 15.

(D3) *The orders of elements of $\mathbb{Z}_n$.* The *order* of an element $[a]_n \in \mathbb{Z}_n$ is the smallest integer k such that adding $[a]_n$ to itself k times yields $[0]_n$, that is $ka \equiv 0 \bmod n$.

(a) Find the order of each element of $\mathbb{Z}_{12}$. Do the same for $\mathbb{Z}_{10}$.
(b) Conjecture a formula for the order of $[a]_n$ in terms of a and n.
(c) Let k denote your conjectured order for $[a]_n$. Prove $[k]_n[a]_n = 0$.
(d) Let k denote your conjectured order for $[a]_n$, and suppose $[c]_n[a]_n = 0$. Prove $k \mid c$.
(e) Prove that your conjectured order formula holds.
(f) For which n does every nonzero $[a]_n$ have order n? Give a (short and sweet) proof.

Homework problems. You must submit *all* homework problems in order to receive full credit.

Unless otherwise stated, $a, b, c, n \in \mathbb{Z}$ are arbitrary, and $n \geq 2$.

(H1) Find all $x, y \in \mathbb{Z}_7$ that are solutions to both of the equations

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

(H2) Prove that an integer a is divisible by 8 if and only if the last three digits of a in base 10 form a 3-digit number that is divisible by 8.

(H3) Prove $(a+b)^5 \equiv a^5 + b^5 \bmod 5$ (this is a special case of the "Freshman's Dream" equation).

(H4) (a) Suppose $(a_n \cdots a_1 a_0)_{10}$ expresses a in base 10. Prove that $13 \mid a$ if and only if

$$13 \mid (a_n \cdots a_1)_{10} + 4a_0.$$

(b) Use part (a) to decide whether 20192018 is divisible by 13.

(H5) Determine whether each of the following is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) If $ac \equiv bc \bmod n$ and $c \not\equiv 0 \bmod n$, then $a \equiv b \bmod n$.

(b) If $ab \equiv 0 \bmod n$, then $a \equiv 0 \bmod n$ or $b \equiv 0 \bmod n$.

(c) If $(a, n) = (b, n)$, then $a \equiv b \bmod n$.

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) Prove or disprove: if $a^2 \equiv b^2 \bmod n$, then $a \equiv b \bmod n$ or $-a \equiv b \bmod n$.