Fall 2018, Math 320: Week 3 Problem Set
Due: Tuesday, September 18th, 2018
Modular Arithmetic

Discussion problems. The problems below should be completed 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 $a \equiv (a_r + \cdots + a_1 + a_0) \bmod 9$.

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

$$\begin{aligned}[a]_9 &= [a_r(\underline{\hspace{1.5em}}) + \cdots + a_2 10^2 + a_1 10 + a_0]_9 \\ &= \underline{\hspace{6em}} \\ &\vdots \\ &= \underline{\hspace{6em}} \\ &= [a_r + \cdots + a_1 + a_0]_9,\end{aligned}$$

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

(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.

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

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

(R1) Determine whether each of the following statements is true or false. Justify your answers. You may *not* use a calculator.

(a) 14323341327 is prime.

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

(R2) Prove that an integer a is divisible by 4 if and only if the last two digits of a in base 10 form a 2-digit number that is divisible by 4.

(R3) Prove $(a + b)^3 \equiv a^3 + b^3 \bmod 3$ (this is a special case of the Freshman's Dream equation).

(R4) Suppose $a \equiv b \bmod n$. Prove $(a, n) = (b, n)$. Does the converse hold?

(R5) Determine whether each of the following is true or false. Give an explanation for each true statement, and a counterexample for each false statement.

(i) If $a \equiv b \bmod n$, then $ac \equiv bc \bmod n$.

(ii) If $ac \equiv bc \bmod n$, then $a \equiv b \bmod n$.

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

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 $(a_n \cdots a_1 a_0)_{10}$ expresses a in base 10. Prove that

$$a \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \bmod 11.$$

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

(S2) (a) Suppose $(a_n \cdots a_1 a_0)_{10}$ expresses a in base 10. Prove that $7 \mid a$ if and only if

$$7 \mid (a_n \cdots a_1)_{10} - 2a_0.$$

(b) Use part (a) to decide whether 20182015 is divisible by 7.

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 that there are infinitely many primes of the form $3k + 2$ for some $k \geq 1$.