Fall 2023, Math 320: Week 3 Problem Set
Due: Thursday, September 21st, 2023
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) $1234567 \cdot 90123 = 111262881731$.
(d) There exists $x \in \mathbb{Z}_4$ such that $x^2 + x = [1]_4$.
(e) The equation $x^2+1 = 0$ has no integer solutions (use **modular arithmetic** to justify).
(f) For each $n \geq 3$, the equation $x^2 + [1]_n = [0]_n$ has no solutions in $\mathbb{Z}_n$.

(D2) *Divisibility rules.* In 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 m, and suppose

$$m = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

is the expression of m in base 10, with $0 \leq a_i \leq 9$ for each i.

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

Proof. Using the above expression for m, we obtain

$$\begin{aligned}
[m]_9 &= [a_r(\underline{\qquad}) + \cdots + a_2 10^2 + a_1 10 + a_0]_9 \\
&= [\underline{\qquad\qquad}]_9 + \cdots + [\underline{\qquad\qquad}]_9 + [a_1 10]_9 + [a_0]_9 \\
&= [\underline{\qquad}]_9[\underline{\qquad\quad}]_9 + \cdots + [\underline{\qquad}]_9[\underline{\qquad\quad}]_9 + [a_1]_9[10]_9 + [a_0]_9 \\
&= [\underline{\qquad}]_9[\underline{\quad}]_9 + \cdots + [\underline{\qquad}]_9[\underline{\quad}]_9 + [a_1]_9[1]_9 + [a_0]_9 \\
&= [\underline{\qquad}]_9 + \cdots + [\underline{\qquad}]_9 + [a_1]_9 + [a_0]_9 \\
&= [a_r + \cdots + a_1 + a_0]_9,
\end{aligned}$$

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

(b) Prove that $9 \mid m$ if and only if the sum of the digits of m is divisible by 9.
(c) Modify your proof in part (a) to prove that an integer m is divisible by 3 if and only if the sum of its digits (in base 10) is divisible by 3.
(d) Prove that $5 \mid m$ if and only if the last digit of m is 0 or 5.
(e) Using parts (c) and (d), 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 $\mathbb{Z}_7$, $\mathbb{Z}_{10}$, and $\mathbb{Z}_{12}$.
(b) Conjecture a formula for the order of $[a]_n$ in terms of a and n.
Hint: use your answers from part (a) for inspiration. When in doubt, do more examples!
(c) Based on your conjectured formula, 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, $a, b, c, d, n \in \mathbb{Z}$ are arbitrary and $p \in \mathbb{Z}_{\geq 2}$ is prime.

(H1) Prove $(a+b)^5 \equiv a^5 + b^5 \bmod 5$ (this is a special case of the "Freshman's Dream" equation).

(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) (a) Suppose

$$m = a_r \cdot 10^r + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

expresses m in base 10. Prove that $13 \mid m$ if and only if

$$13 \mid (a_r \cdot 10^{r-1} + \cdots + a_3 \cdot 10^2 + a_2 \cdot 10 + a_1) + 4a_0.$$

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

(H4) Prove that if $[a]_n[c]_n = [b]_n[c]_n$ and $\gcd(c, n) = 1$, then $[a]_n = [b]_n$.

(H5) The following statements are all **false**. For each, provide a counterexample.

(a) If $ab \equiv 0 \bmod n$, then $a \equiv 0 \bmod n$ or $b \equiv 0 \bmod n$.
(b) If $ac \equiv bc \bmod n$ and $c \not\equiv 0 \bmod n$, then $a \equiv b \bmod n$.
(c) If $\gcd(a, n) = \gcd(b, n)$, then $a \equiv b \bmod n$.
(d) If $n \geq 2$, then $(a + b)^n \equiv a^n + b^n \bmod n$ for every $a, b \in \mathbb{Z}$.

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) Find and prove a characterization of the integers $n \geq 1$ for which the following statement holds for all $a, b \in \mathbb{Z}$: "If $a^2 \equiv b^2 \bmod n$, then $a \equiv b \bmod n$ or $-a \equiv b \bmod n$."