Fall 2022, Math 522: Week 4 Problem Set
Due: Friday, September 30th, 2022
Modular Arithmetic (Week 1)

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) $8642 \cdot 97531 \equiv -1 \bmod 4$.

(e) $1234567 \cdot 90123 = 111262881731$.

(f) There exists $x \in \mathbb{Z}$ such that $x^2 + x \equiv 1 \bmod 2$.

(g) There exists $x \in \mathbb{Z}$ such that $x^3 + x^2 - x + 1 = 1522745$.

(h) The equation $x^2 + 1 = 0$ has no integer solutions.

(i) For each $n \geq 2$, the equation $x^2 + 1 \equiv 0 \bmod n$ has no integer solutions.

(j) For each $n \geq 2$, the integer solutions to $x^2 - 1 \equiv 0 \bmod n$ lie in at most 2 equivalence classes modulo 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 a, and suppose $(a_r \cdots a_1 a_0)_{10}$ is the expression of a in base 10, with $0 \leq a_i \leq 9$ 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

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

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

(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) Prove that $5 \mid a$ if and only if the last digit of a is 0 or 5.

(e) Using parts (c) and (d), develop a criterion for when an integer is divisible by 15.

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

Unless otherwise stated, $a, b, c, n, p \in \mathbb{Z}$ are arbitrary with $p > 1$ prime and $n \geq 2$.

(H1) 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.

(H2) Prove $(a+b)^5 \equiv a^5 + b^5 \bmod 5$ (this is a special case of the "Freshman's Dream" equation).

(H3) (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.

(H4) Prove that if $\gcd(c, n) = 1$, then $ac \equiv bc \bmod n$ implies $a \equiv b \bmod n$.

(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) 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 $-a \equiv b \bmod n$."