Spring 2021, Math 522: Problem Set 4
Due: Thursday, February 25th, 2021
Modular Arithmetic (Week 2)

(D1) *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.

(D2) *Euler's theorem.* Fix $n \geq 1$, and let $s = \phi(n)$ denote the number of integers $i \in [1, n-1]$ with $\gcd(i, n) = 1$ (this is known as the *Euler totient function*). The goal of this problem is to prove the following theorem.

Theorem (Euler's Theorem)**.** *If* $\gcd(a, n) = 1$*, then* $a^s \equiv 1 \bmod n$*.*

(a) A *reduced residue system* for n is a collection of integers $r_1, \ldots, r_s$ such that

- $\gcd(r_i, n) = 1$ for each i,
- $r_i \not\equiv r_j \bmod n$ whenever $i \neq j$, and
- for any $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, we have $a \equiv r_i \bmod n$ for some i.

Locate 2 distinct reduced residue systems for $n = 12$ that share at least one element.

(b) Prove that if $r_1, \ldots, r_s$ is some reduced residue system for n and $\gcd(a, n) = 1$, then $ar_1, \ldots, ar_s$ is also a reduced residue system for n.

Hint: the "cancellation law" should come in handy somewhere in your proof.

(c) What does part (b) tell you about the products $r_1 \cdots r_s$ and $(ar_1) \cdots (ar_s)$ modulo n?

(d) Conclude that Euler's theorem holds.

(e) Use Euler's theorem to prove Fermat's little theorem.

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) Determine how many primes p satisfy $n! + 2 \leq p \leq n! + n$. Prove your claim.

(H2) Prove that $10 \nmid (n-1)! + 1$ for all $n \geq 1$. What does this tell you about the hypotheses for Wilson's theorem?

(H3) Prove that if $\gcd(a, n) = \gcd(a-1, n) = 1$, then $1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \bmod n$.

(H4) Prove that if $p > 1$ is prime, then $(a+b)^p \equiv a^p + b^p \bmod p$ for every $a, b \in \mathbb{Z}$ (this is known as the *Freshmen's Dream*).

Note: you may **not** use the binomial theorem in this problem.

(H5) Write up a full solution to parts (b) through (d) of Problem (D2) from discussion.

(H6) Determine whether each of the following is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) If $\gcd(a, n) = 1$, then the smallest positive b such that $a^b \equiv 1 \bmod n$ is $b = \phi(n)$.

(b) If $n \geq 2$, then $(a+b)^n \equiv a^n + b^n \bmod n$ for every $a, b \in \mathbb{Z}$.