Name: Solutions

Problem 0 (2 points). State the Fundamental Theorem of Arithmetic.

Every integer $n \neq 0, 1, -1$ can be written as a product of primes. This factorization is unique: if $p_1, \dots, p_s, q_1, \dots, q_r$ are primes such that $n = p_1 \cdots p_s = q_1 \cdots q_r$, then $r = s$ and $p_1 = \pm q_1, \dots, p_n = \pm q_n$, up to possibly relabeling the q's.

Problem 1 (4 points). Let a and n be positive integers. Prove that if $[a] = [1] \bmod n$ then $(a, n) = 1$.

By definition, $[a] = [1]$ means that $a = qn + 1$ for some $q \in \mathbb{Z}$. Suppose $d \mid a$ and $d \mid n$. Then $d \mid (a - qn) = 1$, implying $d = \pm 1$. Then ± 1 are the only common divisors of a and n and $(a, n) = 1$.

Problem 2 (4 points). True or false? Justify your answer with a proof if it is true or a counterexample if it is false.

Given positive integers a and n, if $(a, n) = 1$, then $[a] = [1] \bmod n$.

False. Take $a = 2$ and $n = 3$. We do have $(2, 3) = 1$, but $2 \not\equiv 1 \pmod 3$.