

Name:

**Problem 0** (2 points). Which of the statements below *must* be true in any ring?

- (a) Addition is associative.
- (b) Multiplication is associative.
- (c) Addition is commutative.
- (d) Multiplication is commutative.
- (e) Every element has an additive inverse.
- (f) Every non-zero element has a multiplicative inverse.

**Problem 1** (4 points). Prove that if the equation  $ax \equiv b \pmod{n}$  has a solution, then  $(a, n) | b$ .

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

If  $(a, n) = 1$ , then  $[a]$  has a multiplicative inverse in  $\mathbb{Z}_n$ .

**Problem 3** (Bonus). If  $a > b > 2$  are integers, then  $2^b - 1$  does not divide  $2^a + 1$ .