

**EXAM 1**

name: \_\_\_\_\_

1. a. (8 points) Give the definition of the congruence class of  $a$  modulo  $n$  ( $[a]_n$ ).
- b. (12 points) Prove if  $([a]_n)^k = [1]_n$  for some integer  $k > 1$ , then  $(a, n) = 1$ .
2. (a) (12 points) Prove Proposition 1.2.3(a), which says: Let  $a, b$  and  $c$  be non-zero integers. If  $b|ac$ , then  $b|(a, b)c$ .
- (b) (10 points) Let  $x$  and  $y$  be non-zero integers. Prove that if  $(3x, 10y) = 7$ , then  $7|(x, y)$ .
3. a. (8 points) Define relatively prime.
- b. (12 points) Let  $a, n \in \mathbb{Z}$ , with  $n > 1$ . Prove that if  $(a, n) = 1$ , then for any  $[c]_n \in \mathbb{Z}_n$ , there exists an element  $[k]_n \in \mathbb{Z}_n$  such that

$$[a]_n [k]_n = [c]_n.$$

4. a. (8 points) Give the definition of an invertible element in  $\mathbb{Z}_n$ .
- b. (4 points) Give an example of an invertible element of  $\mathbb{Z}_{12}$ .
- c. (4 points) Find all elements in  $\mathbb{Z}_{12}$  satisfying  $[a]_{12} = [a]_{12}^{-1}$ , or equivalently such that  $([a]_{12})^2 = [1]_{12}$ .
- d. (12 points) Let  $p$  be prime. Prove that if  $([a]_p)^2 = [1]_p$ , then  $[a]_p = [1]_p$  or  $[a]_p = [-1]_p$ .
5. Let  $q \in \mathbb{Z}$  with  $q \neq 0$ . Define  $\mathbb{Z}[\frac{1}{q}]$  to be the set of rational numbers such that the denominator is a power of  $q$ . In other words, let

$$\mathbb{Z}[\frac{1}{q}] = \left\{ \frac{n}{q^a} : n, a \in \mathbb{Z}, a \geq 1 \right\}.$$

- (a) (2 points) Give an example of an element of  $\mathbb{Z}[\frac{1}{3}]$  that is not an integer.
- (b) (2 points) Show that  $\mathbb{Z} \subseteq \mathbb{Z}[\frac{1}{3}]$ .
- (c) (6 points) Prove that  $\mathbb{Z}[\frac{1}{q}]$  is closed under addition and multiplication.