

**Time Limit: 50 minutes**

*Score:* \_\_\_\_\_

---

This exam contains 7 pages (including this cover page) and 5 problems. Enter all requested information on the top of this page. It contains 50 points.

This test is closed book and closed note. You are required to show all of your work on each problem on this exam, and provide explanations of your reasoning where asked. The following rules apply:

- Please show all of your work as partial credit will be given where appropriate, and there may be no credit given for problems where there is no work shown.
- For problems that ask you to prove something, you must give a complete proof. Your arguments should be clear, logically ordered, and justification must be given for each non-trivial step.
- For each proof, please **state which proof techniques you are using**. This includes direct, contradiction, contrapositive, and induction proofs.

**Notation:**

- If  $n \in \mathbb{Z}_{>0}$  and  $a, b \in \mathbb{Z}$  then  $a \equiv b \pmod{n}$  means that  $n|(b - a)$ .
- If  $n \in \mathbb{Z}_{>0}$  then  $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$  is the set of integers modulo  $n$ .
- If  $n \in \mathbb{Z}_{>0}$  and  $a \in \mathbb{Z}$  we write  $a \% n$  for the remainder of the Euclidean division of  $a$  by  $n$ . This is unique element of  $\mathbb{Z}_n$  such that  $a \equiv a \% n \pmod{n}$ .

1. (10 points) (a) Find  $\gcd(71, 33)$  using the Euclidean algorithm.

(b) Solve the congruence equation  $33x \equiv 5 \pmod{71}$

2. (10 points) Let  $n$  be a positive integer such that  $n$  has exactly three positive divisors.  
Prove that  $n$  is the square of a prime number.

3. (10 points) Prove that if  $p > 3$  is a prime then  $6 \mid (p^2 - 1)$ .

4. (10 points) (a) Compute  $(3^{47} - 25)\%28$ , that is, find the integer  $x$  with  $0 \leq x < 28$  such that  $3^{47} - 25 \equiv x \pmod{28}$ .

- (b) For which positive integers  $n$  is the statement

$$\forall a \in \{1, \dots, n-1\} \exists x \in \mathbb{Z} : ax \equiv 1 \pmod{n}$$

true?

5. (10 points) Consider the following statement: If  $x, y$  are integers such that  $x \equiv y \pmod{3}$ , then  $x^{3^n} \equiv y^{3^n} \pmod{3^{n+1}}$  for every integer  $n \geq 0$ .

Suppose you are going to prove the statement by induction on the exponent  $n$ .

- (a) Write down the statement that you need to prove for the **base case**, and explain why it is true.

- (b) Write down the statement that needs to proven in the **inductive step** and underline the **inductive hypothesis**.

- (c) Prove the inductive step. *Hint: You may want to use that  $a \equiv b \pmod{3^n}$  if and only if  $a = b + 3^n \cdot k$  for some  $k \in \mathbb{Z}$ .*