Name: _____

PID: _____

Question	Points	Score
1	10	
2	10	
3	10	
4	10	
5	10	
Total:	50	

1. Write your Name, PID, and Section on the front of your Blue Book.
2. Write the Version of your exam on the front of your Blue Book.
3. No calculators or other electronic devices are allowed during this exam.
4. You may use one page of notes, but no books or other assistance during this exam.
5. Read each question carefully, and answer each question completely.
6. Write your solutions clearly in your Blue Book
   (a) Carefully indicate the number and letter of each question.
   (b) Present your answers in the same order they appear in the exam.
   (c) Start each question on a new page.
7. Show all of your work; no credit will be given for unsupported answers.

1. (10 points) Prove that $\sqrt{3}$ is irrational.
2. (10 points) Let $a, b, n \in \mathbb{Z}$. Suppose $a \equiv b \pmod{n}$. Prove that
$$\gcd(a, n) = \gcd(b, n).$$
3. (10 points) Prove that there are infinitely many primes of the form $3k - 1$.
4. (10 points) Find all integers n such that $2^n \equiv 1 \pmod{7}$. Justify your answer.
5. Suppose $[a]_k^n = [1]_k$, $[b]_k^m = [1]_k$, and $\gcd(m, n) = 1$.
   (a) (5 points) Prove that $([a]_k^i)^n = [1]_k$ for any integer i.
   (b) (5 points) Prove that $\{[a]_k^i |\ i \in \mathbb{Z}\} \cap \{[b]_k^j |\ j \in \mathbb{Z}\} = \{[1]_k\}$.

Good Luck!