Name: _____

Student ID: _____

Honor Code: As a member of the UC Berkeley community, I act with honesty, integrity, and respect for others.

Signature: _____

This is a closed-note, closed-book, closed-calculator, etc. exam. Unless otherwise indicated, you can use results proved in lecture, the textbook, and homework, provided they are clearly stated. If necessary, continue solutions on backs of pages.

The exam is out of 40 points, but there are 5 points of bonus credit available, for a maximum possible score of 45.

Time limit: 60 minutes.

Problem	Total Points	Earned Points
1	10	
2	10	
3	10	
4a	10	
4b (Bonus)	Up to 5	
Total	40	

1. (**10 points**) Let S and T be nonempty sets, and $f : S \to T$ a function. Consider the following "left-cancellation property:"

For any set U and any two functions $g_1 : U \to S$, $g_2 : U \to S$, if $f \circ g_1 = f \circ g_2$ as functions $U \to T$, then $g_1 = g_2$.

Prove that f is injective if and only if f satisfies the left-cancellation property. [Hint for one direction: let U be a one-element set.]

2. (**10 points**) Show that for any integer $n \geq 6$, there exist *nonnegative* integers x, y such that $3x + 4y = n$.

3. (**10 points**) Determine, with proof, whether 3^{27} is a quadratic residue mod 41. [Hint: $3^4 = 81$.]

4. Two problems on mod p approaches to Diophantine problems:

4a. (**10 points**) Let $f(x)$ be a polynomial with integer coefficients. Suppose $p_1, \ldots, p_r$ are distinct prime numbers, and suppose that for every $n \in \mathbf{Z}$, $f(n)$ is divisible by at least one of the p_i (this p_i could change depending on n). Show that there must actually be a *single* p_j such that for every $n \in \mathbf{Z}$, $f(n)$ is divisible by p_j. [Hint: proof by contradiction.]

4b. (**Bonus problem, 5 points**) Let $f(x)$ be a quadratic polynomial with integer coefficients. Suppose p is a prime number, and $n \in \mathbf{Z}$ satisfies

$$f(n) \equiv 0 \bmod p, \quad f'(n) \not\equiv 0 \bmod p,$$

where f' is the derivative of f. Show that there is an integer $m \in \mathbf{Z}$ such that $m \equiv n \bmod p$ and $f(m) \equiv 0 \bmod p^2$ (i.e. we may "lift" a root of $f \bmod p$ to a root of $f \bmod p^2$). [Hint: think about $f(n + rp)$ for an integer r.]