

Instructions. Answer each of the questions on your own paper, and be sure to show your work, including giving reasons, so that partial credit can be adequately assessed. Put your name on each page of your paper. There is a total possible of 80 points.

1. [10 Points]

- (a) Compute $\phi(1500)$.
- (b) Determine the remainder when 7^{1203} is divided by 1500. (*Hint:* Euler's Theorem.)

2. [12 Points]

- (a) Give the definition of *congruence modulo m* . That is, complete the following sentence: Integers a and b are congruent modulo m (in notation $a \equiv b \pmod{m}$) if ...
- (b) Use the definition of congruence modulo m from part (a) to prove that if $a \equiv 3 \pmod{4}$ then $a^2 \equiv 1 \pmod{8}$.

3. [12 Points] Use the Chinese Remainder Theorem to solve the following system of simultaneous congruences.

$$\begin{aligned}x &\equiv 2 \pmod{5} \\x &\equiv 4 \pmod{6} \\x &\equiv -5 \pmod{7}\end{aligned}$$

4. [14 Points] Decide whether the following linear congruences are solvable. If so, give the least complete solution, if not say why there are no solutions.

- (a) $15x \equiv 17 \pmod{33}$.
- (b) $21x \equiv 56 \pmod{91}$.

5. [6 Points] Let $f(x)$ be a polynomial with integer coefficients. Assume that $f(x) \equiv 0 \pmod{5}$ has 4 solutions; $f(x) \equiv 0 \pmod{7}$ has 5 solutions; $f(x) \equiv 0 \pmod{3}$ has 2 solutions; and $f(x) \equiv 0 \pmod{4}$ has no solutions. How many solutions does $f(x) \equiv 0 \pmod{m}$ have in each of the following cases:

- (a) $m = 21$;
- (b) $m = 28$;
- (c) $m = 105$;

6. [14 Points]

- (a) Make a list of all the integers between 1 and 18 which are quadratic residues mod 19.
- (b) Using your list in part (a), find a complete solution to the quadratic congruence

$$2x^2 + 2x + 7 \equiv 0 \pmod{19}.$$

7. [12 Points] Let $f(x) = x^3 + x^2 - 5$. Assuming that $x \equiv 2 \pmod{7}$ is the only solution to $f(x) \equiv 0 \pmod{7}$, find all solutions to $f(x) \equiv 0 \pmod{49}$.