Midterm Exam, Wednesday, December 1

Duration: 55 minutes — Calculators are allowed

Remarks: This is a long exam; **do as much of it as you can, and please take care to budget your time wisely.** Each problem is worth ten points; you may do the problems in any order (kindly indicate in your blue book which problem you are solving at any given time).

Please make sure to communicate your ideas by explaining your reasoning precisely and clearly.

GOOD LUCK!

Problem 1. a) Find the prime factorizations of 192 and of 150.

b) Use your answer for part a) to find the GCD $(192, 150)$.

c) Use your answer for part a) to find the sum of the factors of 150.

Problem 2. a) Solve the equation $7x \equiv 1 \pmod{101}$.

b) Find the general solution (with integers x, y) of the equation $22x + 60y = 6$.

Problem 3. a) Find the remainder of 4^{183} mod 61.

b) Find the remainder of 2^{264} mod 25.

c) How many primitive roots are there mod 61?

(Remark: parts (a), (b), and (c) are independent.)

Problem 4. Assume given a and m such that a has order ℓ mod m. Let k be given. Find, with proof, the order (mod m) of a^k.

Problem 5. a) Carefully state the Chinese remainder theorem.

b) Use the Chinese remainder theorem to show that if $(a, 77) = 1$, then $a^{30} \equiv 1 \pmod{77}$.

Problem 6. a) Find a solution of $x^2 \equiv -1 \pmod{5}$.

b) Find a solution of $x^2 \equiv -1 \pmod{25}$.

c) Find a solution of $x^2 \equiv -1 \pmod{125}$.

(Remark: I am not asking you to find the most general solution; just find one particular solution in each case.)

Problem 7. Let p be a prime number, and let k be a number such that $(k, p-1) = 1$. Let a be given (you may assume $a \not\equiv 0 \pmod{p}$ if you like). Show that the equation

$$x^k \equiv a \pmod{p}$$

has exactly one solution $x \pmod{p}$.

(Hint: Either raise the equation to the mth power for a suitable m, or use indices.)