Math 222 Exam 1: Wednesday, February 19 1997; 1:55–2:45pm

Instructions. Use your time wisely; the four questions are not of equal value. To receive full points for the proofs in questions 3 and 4, complete reasons for all steps must be supplied. Calculators may be used if desired.

Throughout the exam, $\mathbf{Z}_m$ denotes the integers modulo m.

1. *(35 points)*

(a) Use the Euclidean algorithm to compute the greatest common divisor d of 13 and 19 and to express it in the form $d = 13a + 19b$ for integers a and b.

(b) Solve the congruence $13x \cong 5 \pmod{19}$.

(c) Evaluate $\overline{5} \cdot \overline{13}^{-1} + \overline{4}$ in $\mathbf{Z}_{19}$.

(d) Find which of the 19 congruence classes in $\mathbf{Z}_{19}$ are squares i.e. of the form $\overline{x}^2$ for some integer x.

2. *(30 points)*

(a) Let R denote a commutative ring. Carefully define the terms "zero divisor in R" and "unit of R."

(b) Give precise descriptions in terms of the integers a and m of when the congruence class $\overline{a}$ in $\mathbf{Z}_m$ is a zero-divisor, and of when it is a unit.

(c) Use your descriptions from (b) to list the zero-divisors and the units of the ring $\mathbf{Z}_{18}$.

(d) Is it true that in any commutative ring R, the sum $a + b$ of units a and b of R is a unit? (Hint; use (c) to look for a counterexample in $\mathbf{Z}_{18}$).

3. *(20 points)*

(a) State the principle of mathematical induction.

(b) Carefully prove the following statement by induction on n; if n is a positive integer, then

$$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + 4 \cdot 2^4 + \ldots + n \cdot 2^n = (n-1) \cdot 2^{n+1} + 2.$$

4 *(15 points)* Let R be a ring, and 0 denote the additive identity of R, defined by the property that $r + 0 = r = 0 + r$ for all elements r of R.

An additive inverse for an element a of R is an element d of R such that $a + d = d + a = 0$. Below, we break down the proof that additive inverses are unique into parts (a)–(c).

Suppose that elements b and c of R are both additive inverses of the element a of R.

(a) Write down the equations expressing the fact that b is an additive inverse of a, and use them to calculate $(b + a) + c$.

(b) Write down the equations expressing the fact that c is an additive inverse of a, and use them to calculate $b + (a + c)$.

(c) Use parts (a) and (b) to prove that $b = c$.