Math 223 Exam 2; April 2, 2004

Instructions for questions 1–4. Answer the questions in the spaces provided. They are worth *5 points each.*

1. Use the Euclidean algorithm to calculate the gcd d of 80 and 35 and express d in the form $d = 80x + 35y$ for integers x and y.

2. Determine the least natural number N such that $2^N \equiv 1 \pmod{25}$.

3. Find a solution of the three simultaneous congruences $x \equiv 1 \pmod{2}$, $x \equiv 3 \pmod{5}$ and $x \equiv 2 \pmod{7}$.

4. Determine all the rational zeros of the polynomial $f(x) = x^3 - 3x^2 + 4$.

Instructions for Questions 5–8 Give careful statements of the indicated definitions, principles or theorems in the spaces provided. These questions are worth *5 points each*. Points will be deducted for unclear or imprecise (or of course incorrect) answers.

5. Give a careful definition of a prime natural number, and state the fundamental theorem of arithmetic.

6. Let $n \geq 2$ be a natural number. Explain what is meant by a congruence class modulo n. How many such (distinct) congruence classes are there?

7. State Fermat's little theorem.

8. Recall the construction of the rational numbers from the integers (involving the set F of ordered pairs of integers (a, b) with $b \neq 0$ under a suitable equivalence relation $\sim$). Describe the appropriate equivalence relation $\sim$ on F explicitly. How is the fraction a/b defined explicitly in terms of F and $\sim$?

Instruction for Questions 9–12 Questions 9–12 are True/False questions worth *5 points each*. Write your answer (T or F) in the space provided. No working is required.

9. The only solutions $x \in \mathbf{Z}$ of the equation $x^2 \equiv 1 \pmod 8$ are $x \equiv 1 \pmod 8$ and $x \equiv -1 \pmod 8$.

Answer:

10. Let $X = [8] = \{1, 2, 3, \ldots, 8\}$. Consider the partition of X into the sets $\{1, 3, 5, 7\}$, $\{2, 4, 6, 8\}$. Then the equivalence relation R on X corresponding to this partition is given by xRy iff $x, y \in X$ and $x - y$ is even.

Answer:

11. The congruence $57x \equiv 1 \pmod{403}$ has a unique solution.

Answer:

12. The set $\mathbf{Z}_n$ of integers modulo n forms a group with binary operation $\circ$ given by $[a] \circ [b] = [ab]$.

Answer:

Instruction for Questions 13–15 Provide careful proofs of the indicated statements in the spaces provided. Points will be deducted for unclear or imprecise explanation.

13. *(15 points)* Prove that there are infinitely many prime numbers.

14. *(10 points)* Prove: if a, b, c are integers such that a and b are relatively prime and a divides bc, then a divides c

15. *(15 points)* Prove that the relation defined on $\mathbf{R} \times \mathbf{R}$ by $(x, y) \sim (a, b)$ if $x^2 + y^2 = a^2 + b^2$ is an equivalence relation.