310 Introduction to Modern Algebra
Instructor: Petronela Radu
July 8, 2009

Sample Problems for the Final Exam

1. Suppose that $a = 6^5 \cdot 7^{11} \cdot 17^2$ and $b = 2^7 \cdot 5^8 \cdot 15^3 \cdot 17^5$. Find (written as a product of prime powers):

   (a) the greatest common divisor (GCD) of a and b:

   (b) the least common multiple (LCM) of a and b:

2. Find $[6]^{-1}$ in $\mathrm{U}(\mathbb{Z}_{13})$ $\quad (= \{[a] \mid \mathrm{GCD}(a, 13) = 1 \text{ and } 0 < a < 13\})$, the group of units of $\mathbb{Z}_{13}$.

3. Define the *greatest common divisor* of two non-zero polynomials $f, g \in \mathbb{Q}[x]$.

4. Find the least non-negative integer solution to each of the following congruences. In (a) and (b) find the *general* solution too. If there is no solution, explain why. (Do *not* use calculators on this problem.)

   (a) $3x \equiv 5 \pmod{10}$.

   (b) $6x \equiv 10 \pmod{12}$.

   (c) $x \equiv 5^{6001} \pmod{7}$.

   (d) $x \equiv 5^{5999} \pmod{7}$.

5. Show that there do not exist integers x and y so that $x^2 + y^2 = 1234567$. (Hint: Write the equality as a congruence modulo 4.)

6. Find, in $(\mathbb{Z}/2\mathbb{Z})[x]$, an irreducible polynomial of degree 3, and explain why it is irreducible. Redo the problem with $(\mathbb{Z}/2\mathbb{Z})[x]$.

7. 9. How many elements x in $\mathbb{Z}/105\mathbb{Z}$ satisfy $x^2 = [1]$? Explain.

8. a. Using the Euclidean Algorithm, find the greatest common divisor d of 2904 and 3210.

   b. Find integers r and s such that $d = 2904r + 3210s$.

9. Use mathematical induction to prove that $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for every integer $n \geq 1$.

   13. Use "Bézout's Identity" to prove Euclid's Lemma: If p is a prime integer and a, b are integers such that $p \mid ab$, then $p \mid a$ or $p \mid b$.

10. Write the list of $\mathrm{U}(\mathbb{Z}/28\mathbb{Z})$, the group of units of $\mathbb{Z}/28\mathbb{Z}$. Underneath each element, list its *order* in $\mathrm{U}(\mathbb{Z}/28\mathbb{Z})$. Show your work, and don't use calculators, except possibly to check your answers.

11. You should not use calculators on this problem, except, perhaps, to check your work. Let $G = \mathrm{U}(\mathbb{Z}/41\mathbb{Z})$, the units of $\mathbb{Z}/41\mathbb{Z}$ with multiplication as the operation. You are given the following information, which you should use freely:

$$3^4 \equiv -1 \pmod{41} \qquad \text{and} \qquad 2^{10} \equiv -1 \pmod{41}.$$

a. Show that the order of [3] is 8 and that the order of [2] is 20.

b. Find a power of [2] whose order is 5.

c. Find an element of order 40. Explain. (Parts a. and b. are helpful here.)

12. Factor $x^7 + x^3 + x + 1$ as a product of irreducible polynomials in $\mathbb{Z}/2\mathbb{Z}$. Explain briefly why each of your factors is irreducible.

13. Find the GCD $d(x)$ of $x^3 + 1$ and $x^7 + 1$ in $\mathbb{Q}[x]$, and find polynomials $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$ such that $d(x) = (x^3 + 1)f(x) + (x^7 + 1)g(x)$.

14. Solve the simultaneous congruences: $x \equiv 32 \pmod{63}, x \equiv 33 \pmod{64}, x \equiv 34 \pmod{65}$.

15. Solve the simultaneous congruences: a. $x \equiv 2 \pmod{6}, x \equiv -3 \pmod{5}, x \equiv 8 \pmod{11}$. b. $x \equiv 22 \pmod{6}, x \equiv 103 \pmod{5}, x \equiv 42 \pmod{11}$.

16. Prove, by induction, that $3^{2n} - 1$ is divisible by 8 for every positive integer n.

17. Let x be an integer relatively prime to 1001 $(= 7 \cdot 11 \cdot 13)$. Prove that $x^{60} \equiv 1 \pmod{1001}$.

18. Find an element of $\mathbb{Z}/1001\mathbb{Z}$ with order 60 (Hint: use previous problem).

19. Prove that $n^9 + 2n^7 + 3n^3 + 4n$ is a multiple of 5, for every integer n.