Name: ____________________

Math 580/780I: Test 3, Fall 2010

Instructions and Point Values: Put your name at the top of this page and at the top of the first page of the packet of blank paper given to you. There are 7 problems below. Work each problem on the paper provided, using a separate page for each problem. Show ALL of your work. Put your answers in the boxes below where appropriate. Do NOT use a calculator.

There are 100 total points possible on this exam. The point value for each problem appears to the left of each problem.

---

14 pts (1) (a) What is the order of 3 modulo 14? Justify your answer.

Order of 3 mod 14: ☐

(b) Is 3 a primitive root modulo 14? Explain your answer.

Answer: ☐ (YES or NO)

---

16 pts (2) Prove the following theorem from class. You should give Euclid's proof by contradiction that was done in class. (The proof should be put in the packet of blank paper.)

Theorem. *There exist infinitely many primes.*

---

12 pts (3) If α_1, α_2, α_3 and α_4 are the roots of the polynomial $x^4 - 3x^3 - 4x^2 + 5x - 7$, then what is the value of

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2\,?$$

Show your work.

Answer: ☐

---

12 pts (4) What is the remainder when we divide

$$x^{2010} - 3\,x^{1999} + x^{1608} - 2\,x^{101} + x^{14} - x^2 + 1$$

by $x^3 + 1$? Show appropriate work.

Remainder: ☐

---

12 pts (5) Calculate $\gcd\left(x^6 - x^4 + 2\,x^3 - 2\,x^2 - x + 1,\ x^5 - x^3 + x^2 - 2\,x + 1\right)$.

gcd:

---

14 pts (6) (a) The number 3 is a primitive root modulo 38. What is the order of 3 modulo 38?

Order of 3 **mod** 38**:**

(b) Find an integer $a \in \{1, 2, \dots, 37\}$ that has order 6 modulo 38. Justify your answer. (Hint: This is similar to a practice problem we did for review.)

a **with order** 6 **mod** 38**:**

---

20 pts (7) (a) If p is a prime and k is a positive integer dividing $p - 1$, then there are exactly $(p-1)/k$ different kth powers modulo p in the set $\{1, 2, 3, \dots, p-2, p-1\}$. How many different 7th powers are there modulo 29 in the set $\{1, 2, 3, \dots, 27, 28\}$?

Number of 7th powers mod 29**:**

(b) Calculate 2^7 modulo 29.

2^7 **mod** 29**:**

(c) What are all the 7th powers modulo 29 in the set $\{1, 2, 3, \dots, 27, 28\}$? (This should be quick if you did part (a) and (b) correctly, but you need to think about the problem in the right way.)

All 7th powers mod 29**:** (List numbers in $\{1, 2, 3, \dots, 27, 28\}$.)