Math 580/780I Review Sheet for Test 3

Stuff to Know:

- The Euclidean algorithm for polynomials.
- How to find $u(x)$ and $v(x)$ such that $f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x))$.
- The elementary symmetric functions.
- The Remainder Theorem.
- Arithmetic modulo polynomials.
- The proof of Theorem 16.
- Proof 1 of Theorem 17.
- The statement of Lagrange's Theorem (Theorem 18).
- How to compute orders of integers modulo some integer $n > 0$.
- How to determine if a number is a primitive root modulo a prime (or integer).
- How to do the quiz problems and the review problems below.
- How to do homework problems and examples from class. This includes items not mentioned above. See class presentations for examples.

Practice Problems:

1. If α_1, α_2 and α_3 are the roots of $x^3 + 2x^2 - 3x + 5$, then what are the values of

$$\alpha_1 + \alpha_2 + \alpha_3, \qquad \alpha_1^2 + \alpha_2^2 + \alpha_3^2, \qquad \text{and} \qquad \alpha_1^3 + \alpha_2^3 + \alpha_3^3\,?$$

2. What is the remainder when we divide

$$x^{2010} + 2x^{2005} + 4x^{1020} - 16x^{1010} + x^{24} - 2x^{12} + x^7 - x^3 + 1$$

by $x^5 + 2$?

3. Let p be a prime $\equiv 5 \pmod 8$, so $p = 8k + 5$ for some integer k. Explain why $x^4 + 1 \equiv 0 \pmod p$ has no solutions.

4. Prove that there are infinitely many primes $\equiv 3$ modulo 4.

5. (a) State Lagrange's Theorem.

   (b) If p is a prime $\equiv 1$ modulo 3, then it is known that each cube x modulo p satisfies the congruence $x^{(p-1)/3} \equiv 1 \pmod{p}$. What does Lagrange's Theorem imply about the number of cubes modulo such a prime?

6. (a) Which of the following can be the order of an integer a modulo 50? There may be more than one correct answer. Find all of them.

$$2, \quad 4, \quad 5, \quad 10, \quad 15, \quad 20, \quad 25$$

   (b) The number 3 is a primitive root modulo 50. Find an integer $a \in \{1, 2, \ldots, 49\}$ that has order 5 modulo 50. If you didn't use that 3 is a primitive root modulo 50, figure out how to.

7. Is 2 a primitive root modulo 23? How about modulo 29?

8. The following are consecutive powers of 5 modulo 37 that your professor has kindly provided for you:

$$5^{24} \equiv 26 \pmod{37}, \quad 5^{25} \equiv 19 \pmod{37}, \quad 5^{26} \equiv 21 \pmod{37},$$
$$5^{27} \equiv 31 \pmod{37}, \quad 5^{28} \equiv 7 \pmod{37}, \quad 5^{29} \equiv 35 \pmod{37},$$
$$5^{30} \equiv 27 \pmod{37}, \quad 5^{31} \equiv 24 \pmod{37}, \quad 5^{32} \equiv 9 \pmod{37}.$$

   In particular, note that $5^{31} \equiv 24 \pmod{37}$. There is an integer $k \in \{1, 2, 3, \ldots, 36\}$ satisfying $k^7 \equiv 24 \pmod{37}$. Find that value of k. (Hint: By Fermat's Little Theorem, $5^{36} \equiv 1 \pmod{37}$ so $5^{67} \equiv 5^{31} \equiv 24 \pmod{37}$. Find the right power of 5 that is congruent to 24 modulo 37.)