Comprehensive Exam: Math 780 & 784

Instructions: There are nine problems below (turn the sheet over for two of the problems). Answer as many as you can on the blank pages provided with this test. You may keep the questions when you are through.

1. Let m_1, m_2, b_1, and b_2 be positive integers. Set $d = \gcd(m_1, m_2)$. Prove that the system of congruences
$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \end{aligned}$$
has an integer solution if and only if $b_1 \equiv b_2 \pmod{d}$.

2. Let $a > 1$ be an integer and let p be an *odd* prime number.
   (i) Let q be a prime number such that q divides $a^p - 1$. Prove that the order of a modulo q is either 1 or p.
   (ii) Explain why either $q|(a-1)$ or $q \equiv 1 \pmod{2p}$.
   (iii) Prove that there are infinitely many primes which are 1 modulo $2p$.

3. Let p be a prime, and let h and k be nonnegative integers such that $h + k = p - 1$. Prove that
$$h!k! + (-1)^h \equiv 0 \pmod{p}.$$

4. Let $n > 1$ be an integer such that $p = 2^n + 1$ is a prime number.
   (i) Prove that 3 is a primitive root modulo p.
   (ii) Let a be a quadratic non-residue modulo p. Prove a is a primitive root modulo p.

5. Let a and b be positive integers. Set $d = \gcd(a, b)$. Prove
$$\gcd(2^a - 1, 2^b - 1) = 2^d - 1.$$

6. Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{-7})$. Explain why R is Euclidean.

7. For the following, $f(x) = x^3 - 10$ and α is a root (any root) of $f(x)$.
   (a) Find a polynomial $g(x)$ that has $3/(\alpha - 1)$ as a root.
   (b) Is $\{1, \alpha, \alpha^2\}$ an integral basis for the ring of algebraic integers in $\mathbb{Q}(\alpha)$? Justify your answer. (Hint: You should be able to see quickly that $\Delta(1, \alpha, \alpha^2)$ is not squarefree. This means that its value cannot be used in the obvious way to answer this question, regardless of the answer. I suggest instead thinking about what part (a) has to do with the question.)

8. Let p be a rational prime, and suppose that there is a positive rational integer $a < p/2$ such that $a^2 \equiv -5 \pmod{p}$. For example, if $p = 7$, then $a = 3$; and if $p = 29$, then $a = 13$. Let R be the ring of integers in $\mathbb{Q}(\sqrt{-5})$.

   (a) Prove the following ideal factorization holds in R:

$$(p) = \big(a + \sqrt{-5}, p\big)\big(a - \sqrt{-5}, p\big).$$

   (b) What is the norm of the ideal $\big(a + \sqrt{-5}, p\big)$ in R? Justify your answer.

   (c) Is $\big(3+\sqrt{-5}, 7\big)$ a prime ideal? Is $\big(13+\sqrt{-5}, 29\big)$ a prime ideal? Justify your answers.

   (d) Is $\big(3 + \sqrt{-5}, 7\big)$ a principal ideal? Is $\big(13 + \sqrt{-5}, 29\big)$ a principal ideal? Justify your answers.

   (e) Is $\big(2 + \sqrt{-5}, 7\big)$ a principal ideal? Justify your answer.

9. Find (with proof) all integers x and y such that $y^2 + 1 = x^5$. (Note that the case that y is odd should be easy.)