Math 109 Spring 1999 Practice Final Examination

1. Define the sequence \( F_n \) for \( n = 0, 1, 2, \ldots \) by \( F_0 = 1, F_1 = 1 \) and \( F_{n+2} = F_{n+1} + F_n \) for \( n \geq 0 \). Thus \( F_2 = F_0 + F_1 = 1 + 1 = 2, F_3 = 2 + 1 = 3 \) and \( F_4 = 3 + 2 = 5 \). Prove that if \( n \geq 2 \) then \( F_n < 2^n \) by induction on \( n \).

2. Prove the following formulas
   \[ a) \ 1 + 3 + 6 + \ldots + \frac{n(n+1)}{2} = \frac{n(n+1)(n+2)}{6}, \]
   \[ b) \ 1 + 4 + 10 + \ldots + \frac{n(n+1)(n+2)}{6} = \frac{n(n+1)(n+2)(n+3)}{24}. \]

   Observe that \( 2 = 1 \cdot 2, 6 = 1 \cdot 2 \cdot 3 \) and \( 24 = 1 \cdot 2 \cdot 3 \cdot 4 \). What is the pattern that a) and b) suggest?

3. Let \( S \) be a set. Prove that if \( S \) is finite then there cannot exist a function \( f: \mathbb{N} \to S \) that is one to one.

4. Let \( F \) be a field. Define for \( m \in \mathbb{N} \), and \( x \in F \), \( m \cdot x \) as follows \( 1 \cdot x = x \) and \( (n+1) \cdot x = n \cdot x + x \). (Thus \( 3 \cdot x = x + x + x \).) Let \( S = \{m \in \mathbb{N}; m \cdot 1 = 0\} \). Prove that if \( F \) is finite then \( S \neq \emptyset \) and there exists a prime \( p \) such that \( S = \{mp; m \in \mathbb{N} \} \). (Hint: Prove that \( n \cdot 1 + m \cdot 1 = (n + m) \cdot 1 \) and \( (n \cdot 1)(m \cdot 1) = (nm) \cdot 1 \). If \( S = \emptyset \) then the function \( f: \mathbb{N} \to F, f(n) = n \cdot 1 \) is one to one since if \( n > m \) and \( m \cdot 1 = n \cdot 1 \) then \( (n - m) \cdot 1 = 0 \). Let \( p \) be the smallest element in \( S \). Now use division with remainder.)

5. Use problem 4. to prove that if \( F \) is a field with four elements \( 0, 1, x, y \) then \( p = 2 \). Use this to write out the addition and multiplication table for \( F \).

6. Let \( a, b \in \mathbb{N} \) be relatively prime (if \( n \in \mathbb{N} \) divides both \( a \) and \( b \) then \( n = 1 \)). Prove that if \( m \in \mathbb{Z} \) then there exist \( r, s \in \mathbb{Z} \) such that \( ra + bs = m \). Is this true if we don’t assume that \( a \) and \( b \) are relatively prime? (You must back up your answer with an explanation.)

7. Use the Euclidean algorithm to calculate the greatest common divisor of each of the following pairs.
   a) 456, 259.
   b) 264, 76.

8. Let \( f(x) = x^4 + 8x^3 + 14x^2 - 8x - 15 \) and \( g(x) = x^3 + 4x^2 - 7x - 10 \) be in \( \mathbb{Q}[x] \). Use the Euclidean algorithm to find the greatest common divisor of \( f(x) \) and \( g(x) \).
9. Prove that the polynomial \( f(x) = x^2 - 3 \) is irreducible as an element of \( \mathbb{Q}(\sqrt{2}) \).
   a) Prove that the set \( F = \{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}; a, b, c, d \in \mathbb{Q} \} \) is a subfield of \( \mathbb{R} \) of degree 4 over \( \mathbb{Q} \).
   b) Let \( \alpha = \sqrt{2} + \sqrt{3} \) prove that \( F = \{ a + b\alpha + c\alpha^2 + d\alpha^3; a, b, c, d \in \mathbb{Q} \} \).
   c) Show that if \( g(x) = x^4 - 10x^2 + 1 \) then \( g(\alpha) = 0 \).
   d) Show that \( F \) is a splitting field for \( g(x) \) over \( \mathbb{Q} \). (Hint: Prove that \( g(x) = ((x - \sqrt{2})^2 - 3)((x + \sqrt{2})^2 - 3).) \)

10. Let \( f(x) = x^2 - 2x + 1 \in \mathbb{Q}[x] \). If \( a(x) \) and \( b(x) \) are in \( \mathbb{Q}[x] \) and if \( a(x) - b(x) \) is divisible by \( f(x) \) then we write \( a(x) \equiv b(x) \mod f(x) \). Prove that is relation is an equivalence relation. Show that if \( a(x), b(x), u(x), v(x) \in \mathbb{Q}[x] \) are such that \( a(x) \equiv u(x) \mod f(x) \) and \( b(x) \equiv v(x) \mod f(x) \) then \( (a(x) + b(x)) \equiv (u(x) + v(x)) \mod f(x) \) and \( a(x)b(x) \equiv u(x)v(x) \mod f(x) \). We will write \([a(x)]\) for the equivalence class of \( a(x) \). Define \([a(x)] + [b(x)]\) to be \([a(x) + b(x)]\) and \([a(x)][b(x)]\) to be \([a(x)b(x)]\). Let \( R \) denote the set of all equivalence classes of \( \mathbb{Q}[x] \) with respect to this equivalence relation. Show that if we take \( 0 = [0] \) then \( R \) is a ring. Show that \( R = \{ [a + bx]; a, b \in \mathbb{Q} \} \). Prove that if \( a, b \in \mathbb{Q} \) and \( a + bx \neq c(x - 1) \) (with \( c \in \mathbb{Q} \)) then there exists \( u \in R \) so that \( u[a + bx] = [1] \).