Finite Fields

1. Use the Euclidean division algorithm (EDA) to determine the gcd of 6711 and 831. Express the gcd as a linear combination $u \cdot 6711 + v \cdot 831$ of 6711 and 831.

2. Find the inverse of 7 modulo 13 using the EDA.

3. Identify all primitive elements of the finite fields of size 7 and 13 (the finite field of size 13 is the set of all integers modulo 13).

4. Over $GF(2)$, compute if possible, the inverse of $(1 + x)$ modulo $(1 + x + x^2 + x^3 + x^4)$.

5. Let $\alpha$ be a primitive element of $GF(64)$. Identify all the elements in all the subfields of $GF(64)$ in terms of $\alpha$.

6. Use the irreducible polynomial (irreducible over $GF(5)$) $x^2 + x + 2$ to construct a finite field of 25 elements. If $\alpha$ denotes a root of $x^2 + x + 2$, then $\alpha$ is known to be primitive in $GF(25)$. Set up an add-1 table for $GF(25)$. Find the minimal polynomials of all elements in the field. Compute the product of all the minimal polynomials (each distinct polynomial is taken just once) including the minimal polynomial of the zero element. Which powers of $\alpha$ constitute the subfield $GF(5)$ of $GF(25)$?

7. Let $\alpha$ be a primitive element of $GF(2^6)$. Identify all the correct answers below with a $\sqrt{\phantom{a}}$:
   - $\alpha + \alpha^4 \in GF(4)$
   - $\alpha + \alpha^8 \in GF(8)$
   - none of the above

8. The polynomials over $GF(2)$ given below are all irreducible. Identify with a $\sqrt{\phantom{a}}$, all those having the property that all of their zeros are contained in $GF(256)$.
   - $x^2 + x + 1$
   - $x^3 + x^2 + 1$
   - $x^4 + x^3 + 1$
   - $x^5 + x^2 + 1$
   - $x^6 + x + 1$
   - $x^8 + x^6 + x^5 + x^4 + 1$
9. Use the irreducible polynomial (irreducible over $\mathbb{F}_3$) $x^2 + x + 2$ to construct a finite field of 9 elements. If $\alpha$ denotes a root of $x^2 + x + 2$, then $\alpha$ is known to be primitive in $\mathbb{F}_9$.

(a) Set up an add-1 table for $\mathbb{F}_9$.
(b) Find the minimal polynomials of all elements in the field.

10. Use the Möbius inversion formulae to determine the number of irreducible polynomials of degree 12 over the binary field $\mathbb{F}_2$.

11. If $\alpha, \beta$ in $\mathbb{F}_{16}$ have orders $a, b$, then is it always true that $\alpha \beta$ has order = $\text{lcm}(a, b)$? Justify your answer.