E2 205 Error-Control Coding
Homework 6

1. Use the Euclidean division algorithm to determine the *gcd* of 6711 and 831. Express the *gcd* as a linear combination $u * 6711 + v * 831$ of 6711 and 831.

2. Over $\mathbb{F}_2$, compute if possible, the inverse of $(1+x)$ modulo $(1+x+x^2+x^3+x^4)$.

3. Identify all primitive elements of the finite fields of size 7 and 13.

4. Let α be a primitive element of $GF(64)$. Identify all the elements in all the subfields of $GF(64)$ in terms of α.

5. Identify the 3-cyclotomic cosets modulo 26 as well as the 2-cyclotomic cosets modulo 19.

6. Let α be a primitive element of $GF(2^6)$. Identify all the correct answers below with a $\surd$
   - $\alpha + \alpha^4 \in GF(4)$
   - $\alpha + \alpha^8 \in GF(8)$
   - none of the above

7. If α, β 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.

8. The polynomials over $GF(2)$ given below are all irreducible. Identify with a $\surd$, 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 α denotes a root of x^2+x+2, then α is known to be primitive in $\mathbb{F}_9$.
   (a) Set up an add-1 table for $\mathbb{F}_9$.
   (b) Identify the 3-cyclotomic cosets modulo 8.
   (c) Find the minimal polynomials of all elements in the field.

10. Is $\mathbb{F}_2[x]/(x^4+x^3+x^2+1)$ a field ? Explain your reasoning as fully as possible.

11. The elements α, β in $\mathbb{F}_{2^6}$ have orders 21 and 9 respectively. Identify as a function of α and β, a primitive element of $\mathbb{F}_{2^6}$.

12. How many binary irreducible polynomials of degree 5 are there ?

13. Identify all the finite fields that are subfields of $\mathbb{F}_{2^{12}}$. If α in $\mathbb{F}_{2^{12}}$ is primitive, identify as a function of α, a primitive element for each of these subfields.

14. Identify the smallest finite field of characteristic 2 that contains a primitive 17-th root of unity.

15. In the notation used in class with regard to finite field Fourier transforms, let $q = 2$, $N = 15$ and α be a primitive element of F_{16} satisfying $\alpha^4 + \alpha + 1 = 0$. Let

$$(s(t),\ t = 0, 1, 2, \ldots, 14) \ = \ 000110000101101 \ .$$

Compute the Fourier transform $\hat{s}(\lambda)$ of $s(t)$. Compute also the Fourier transform of $s(t) + s(t+2)$.