Name and UNI:

Making, Breaking Codes, HW 9

Recall that the book uses the notation $GF(p^d)$ where we use the notation $\mathbf{F}_{p^d}$.

1. Using the Euclidean algorithm compute the gcd of $X^9 + 1$ and $X^5 + 1$ in $\mathbf{F}_2[X]$.

2. Factor $X^6 + 1$ in $\mathbf{F}_2[X]$, i.e., write this polynomial as a product of powers of irreducible polynomials.

3. Counting polynomials.
a. How many polynomials P are there of degree d in $\mathbf{F}_2[X]$?
b. How many polynomials P are there of degree d in $\mathbf{F}_2[X]$ such that $P(0) = 0$?
c. How many polynomials P are there of degree d in $\mathbf{F}_2[X]$ such that $P(1) = 0$?
d. How many polynomials P are there of degree d in $\mathbf{F}_2[X]$ which do not have a root? (In other words, where $P(0) \neq 0$ and $P(1) \neq 0$ in $\mathbf{F}_2$.)
e. Check your answers by listing the polynomials from a., b., c., and d. for $d = 2$.

4. Elliptic curves in characteristic 2.
a. How many points does the elliptic curve $E : y^2 + xy + y = x^3 + x + 1$ have over $\mathbf{F}_2$?
b. How many points does the elliptic curve $E : y^2 + xy + y = x^3 + x + 1$ have over $\mathbf{F}_{2^2} = GF(4)$?

5. On the elliptic curve $E : y^2 = x^3 + x + 12 \bmod 13$ consider the point $P = (1, 1)$. Compute $2P$ and $3P$ in the group law of E. (Double check your points lie on E.)

6. The polynomial $P = X^{10} + X^3 + 1$ is irreducible in $\mathbf{F}_2[X]$. Thus we get $\mathbf{F}_{2^{10}}$ by working modulo P in $\mathbf{F}_2[X]$. Why is it easy to compute the inverse of X^3 modulo P and what is it? (Hint: look at the shape of P.)