ASSIGNMENT #2 FOR CODING THEORY

Instruction. It is *okay* to discuss the problems with your friends, but *you should be by yourself when you write up the solutions.* This is to prevent the situation that you end up "dictating" your friend's explanation without really digesting it.

You should present all the steps in each questions. You may assume without proof all the results covered in the lectures, provided that

- you clearly state the result you're using, and
- the result you assume is not a mere paraphrasing of the question itself.

I. Let F be a field with $q = 2^n$ elements. For any non-zero element $\beta \in F$ we define

$$\mathrm{ord}(\beta) := \min\{i \text{ such that } \beta^i = 1\}.$$

From now on, set $0 \neq \beta \in F$.

(1) Show that $\mathrm{ord}(\beta)$ divides $q - 1$.
(2) Show that β is a primitive element if and only if $\mathrm{ord}(\beta) = q - 1$.
(3) For any integer $d \geq 1$ show that

$$\mathrm{ord}(\beta^d) = \frac{\mathrm{lcm}(\mathrm{ord}(\beta), d)}{d},$$

where $\mathrm{lcm}(a, b)$ means the least common multiple of a and b.
(4) Assume that β is a primitive element. Show that β^d is a primitive element if and only if $\mathrm{hcf}(d, q-1) = 1$.
(5) Now assume that $q = 2^4$ and $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$. Find all primitive elements in F. (*Hint*: First, show that $\alpha \in F$ is a primitive element.)

II. Let $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$. For this question, "minimal polynomials" means minimal polynomials over $\mathbb{B}$.

(1) Find the minimal polynomial of each element of F. (*Hint*: You do *not* have to compute the minimal polynomials 16 times!)
(2) Factorise *all* the polynomials which are minimal polynomials of some $\beta \in F$ into linear polynomials with coefficients in F. (*Remark*: You can solve this problem *without* doing any computation!)
(3) Using *Fermat's little theorem*, factorise $X^{16} - X$ into linear polynomials with coefficients in F.
(4) Combining all the previous parts, factorise $X^{16} - X$ into *irreducible* polynomials in $\mathbb{B}[X]$.

III. Is $\mathrm{BCH}(4, 3)$ r-perfect for any r?

Challenge Problem. This problem will *not* be assessed, though you are invited to submit your solution if you'd like me to comment on it.

Let F be any field with $q = 2^n$ elements. As in the previous question, "minimal polynomials" means minimal polynomials over $\mathbb{B}$.

(1) For $\beta \in F$, let m be the smallest positive integer such that $\beta^{2^m} = \beta$. (This exists by Fermat's little theorem.) Show that the minimal polynomial of β is $\prod_{i=0}^{m-1}(X - \beta^{2^i})$. (*Hint*: Why does all the coefficients of the polynomial $\prod_{i=0}^{m-1}(X - \beta^{2^i})$ belong to $\mathbb{B}$?)
(2) Show that the degree of the minimal polynomial of β divides n. (*Hint*:It follows from (1) that m as in (1) is the degree of the minimal polynomial.)
(3) Let $f(X) \in \mathbb{B}[X]$ be *any* irreducible polynomial of degree m such that $m|n$. Show that $f(X)$ divides $X^{2^n} - X$.
(4) Show that $X^{2^n} - X$ is the product of *all* distinct irreducible polynomials in $\mathbb{B}[X]$ with degree divisible by n. (*Hint*: formal derivative.)