Midterm assignment.

The solutions are to be written in English or Norwegian and delivered to the Rudakov postbox on the 7th floor **by 15:00, March 10**, 2006. Pages of the paper are to be fixed together.
In the paper you **should not write your name**, but write your **student number**.

Each task will be evaluated as a whole, questions marked by letters are not considered separate tasks.

Task 1.

Let $f(x) = x^N - 1$, $g(x) = x^M - 1$ polynomials over $\mathbb{F}_{127}$.
(a) What is the necessary and sufficient condition (on N, M) that g divides f? Why? Explain.

Let $F = 2^k - 1$, $G = 2^l - 1$.
(b) What is the necessary and sufficient condition (on k, l) that G divides F ? Why? Explain.

Let $N = 2^{3^n-1} - 1$, $M = 2^{3^m-1} - 1$ and $f(x) = x^N - 1$, $g(x) = x^M - 1$ as above.
(c) What is the necessary and sufficient condition (on n, m) that g divides f?

Task 2.

We are looking for codes $C \subset \mathbb{F}_3^{80}$ with minimal distance $d \geq 4$ and $k = \dim C$ as large as possible.

(a) Apply the Gilbert-Varshamov theorem to this situation.
How large k can you get from the theorem?
(b) Apply the BCH construction method to this situation.
How large k can you get from the method?
(c) Could it be that in (b) one gets larger k that in (a)?
Would it contradicts the Gilbert-Varshamov theorem or not, why?

Task 3.

Consider $\mathbb{F}_{16}$ made as $\mathbb{F}_2[x]/(h)$ with $h(x) = x^4 + x^3 + 1$, and $\beta = [x]$.
(a) Is β a primitive elements of $\mathbb{F}_{16}$? How you check this?

Let $C \subset \mathbb{F}_2^{15}$ be a code defined by the condition:

$$f_w(\beta^3) = f_w(\beta^7) = 0.$$

(b) What is the dimension of the code C?

We plan to use C and our goal is to correct 1 error and detect as many as possible?
(c) How many errors can be detected?
(d) Describe how the encoding and decoding/detections procedures can.

Task 4.

We can transform a code C over $\mathbb{F}_{31}$ to a binary code $\widetilde{C}$ using binary notations for numbers between 0 and 31.
(a) Use the Reed-Solomon construction and this transformation to make a binary code $\widetilde{C}$ that would correct rare bursts of errors of length up to 13 and have the information rate as large as possible.
(b) Is $\widetilde{C}$ a linear code? If "yes", why, if "no", why?
(c) Count the number of codewords (elements) in $\widetilde{C}$.