Teorema del polinomio generador

Sea C un código cíclico de dimensión k y longitud n, y sea $g(x)$ su polinomio generador. Probar que:

1. C está formado por los múltiplos de $g(x)$ de grado menor que n:

$$C = \{p(x) : gr(p) < n \wedge g(x)|p(x)\}$$

2. $C = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$
3. $gr(g(x)) = n - k$
4. $g(x)|(1 + x^n)$

Para ello, veamos punto a punto.

1. y 2.

Tenemos que demostrar que:

- C está formado por los múltiplos de $g(x)$ de grado menor que n: $C = \{p(x) : gr(p) < n \wedge g(x)|p(x)\}$
- $C = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$

Consideremos $C_1 = \{p(x) : gr(p) < n \wedge g(x)|p(x)\}$ y $C_2 = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera}\}$

Sabemos que un código cíclico es un **ideal**. Es decir, que sea C un código cíclico, $w \in C$ y v una palabra cualquiera, entonces $v \odot w \in C$.
Como en C_2 tenemos que $g(x) \in C$, luego, por la anterior propiedad, $v(x) \odot g(x) \in C$. Por ello mismo, entonces, $C_2 \subseteq C$ $[P1]$.

Sea $p(x) \in C$, consideramos que se divide $p(x)$ por $g(x)$ obteniendo $q(x), r(x) : gr(r) < gr(g) \wedge p(x) = q(x)g(x) + r(x)$. Dado esto, veamos:

$$r(x) = p(x) + q(x)g(x) \text{ ya que estamos en } Z_2$$

$$r(x) = r(x)\ mod(1 + x^n) \text{ ya que } gr(r) < gr(g) < n$$

$$p(x) = p(x)\ mod(1 + x^n) \text{ ya que } gr(p) < n \text{ porque } p(x) \in C$$

Luego, podemos considerar que:

$$
\begin{aligned}
r(x) &= r(x)\ mod(1+x^n) \text{ por lo visto antes} \\
&= [p(x)+q(x)g(x)]\ mod(1+x^n) \text{ reemplazando} \\
&= p(x)+[q(x)g(x)\ mod(1+x^n)] \text{ por lo visto antes} \\
&= p(x)+q(x)\odot g(x) \text{ por def. de } \odot
\end{aligned}
$$

Ahora, como $p(x)\in C, q(x)\odot g(x)\in C$ y C es lineal, entonces $r(x)\in C$.
Sin embargo, como $gr(r)<gr(g)$ que es el polinomio *no nulo* de *menor* grado de C, entonces $r=0$.
Luego, esto significa que $p(x)=q(x)g(x)+r(x)=q(x)g(x)$, lo cual, por definición, está en C_1.
Por ello, entonces, llegamos a que $C\subseteq C_1\ [P2]$.

Ahora, viendo el mismo $p(x)\in C_1$, si aplicamos módulo a la última igualdad tenemos que $p(x)=q(x)g(x)\ mod(1+x^n)=q(x)\odot g(x)$. Luego, por definición, podemos ver entonces que $p(x)\in C_2$, por lo que $C_1\subseteq C_2\ [P3]$.

Luego, entonces, como por $[P1],[P2],[P3]$ tenemos que $C_2\subseteq C, C\subseteq C_1, C_1\subseteq C_2$, entonces llegamos a que $C=C_1=C_2$ demostrando las primeras dos partes.

3.

Tenemos que demostrar que:

- $gr(g(x))=n-k$

Sea t el grado de $g(x)$, por (1) sabemos que $p(x)\in C$ sii es de la forma $q(x)g(x)$ para algún polinomio $q(x)$.
Como el grado de los elementos de C es menor que n, entonces $gr(q(x)g(x))<n$. Luego, $gr(q(x))<n-t$.
Por lo tanto, entonces, la cardinalidad de C es igual a la cantidad del conjunto de polinomios de grado menor que $n-t$. Como tenemos 2^{n-t} posibles polinomios y como C es lineal y su cardinalidad es 2^k, llegamos a que $n-t=k$.
Luego, $t=n-k$ demostrando este punto.

4.

Tenemos que demostrar que:

- $g(x)|(1+x^n)$

Dividimos $(1+x^n)$ por $g(x)$ obteniendo $q(x), r(x)$ con $gr(r)<gr(g)<n$ tal que $1+x^n=q(x)g(x)+r(x)$.
Por ello, $r(x)=1+x^n+q(x)g(x)$
Ahora, como $gr(r)<n$, tenemos que $r(x)=r(x)\ mod(1+x^n)$ y como $0=(1+x^n)\ mod(1+x^n)$, llegamos a que $r(x)=q(x)g(x)\ mod(1+x^n)=q(x)\odot g(x)$
Luego de esto, vemos que coo $r(x)=q(x)\odot g(x)$, por (2) tenemos que $r(x)\in C$. Sin embargo, como $r(x)<g(x)$ y g es el polinomio *no nulo* de menor grado, entonces $r=0$.

Esto significa que $1+x^n = q(x)g(x) + r(x) = q(x)g(x)$, por lo que $g(x)|(1+x^n)$. Luego, se demuestra este punto.