Álgebra III
Semana 10

Alejandro García Montoro
agarciamontoro@correo.ugr.es

17 de enero de 2016

Ejercicio 1. *Función totiente de Euler.*

Apartado 1.1. Prueba que si $p = 2^k + 1$, con $k \in \mathbb{N}$, es un entero primo positivo, entonces k es una potencia de dos. Estos números primos se llaman **primos de Fermat.**

Solución. Demostrémoslo por reducción al absurdo. Supongamos que k no es una potencia de dos; es decir, k tiene al menos un factor primo impar. Llamemos a tal factor, $s > 2$.

Evidentemente, de aquí tenemos que $k = rs$, con $1 \leq r < k$.

En general sabemos que para cualesquiera $a, b \in \mathbb{R}$, y para cualquier $n \in \mathbb{N} - 0$, se tiene que $(a - b)|(a^n - b^n)$.

Si tomamos $a = 2^r$, $b = -1$ y $n = s$, tenemos que $(2^r + 1)|(2^{rs} - (-1)^s)$. Como hemos tomado s impar y $k = rs$, concluimos que:

$$(2^r + 1)|(2^k + 1)$$

Pero de aquí se deduce, puesto que $1 < 2^r + 1 < 2^k + 1$, que $2^k + 1$ no es primo, lo que cae en contradicción con las hipótesis del ejercicio.

Por tanto, k es una potencia de dos.

Apartado 1.2. Prueba que $\varphi(n)$ es una potencia de 2 si, y sólo si, $n = 2^s p_1 \cdots p_t$, con $s \in \mathbb{N}$, y los p_i primos de Fermat, distintos dos a dos.

Solución. Sea $n = 2^s p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ la factorización en números primos de n, con p_i números primos impares, $e_i \geq 1$ y $a \geq 0$. Por la fórmula de φ, tenemos que

$$\varphi(n) = \begin{cases} 2^{s-1}(p_1 - 1)p_1^{e_1-1}(p_2 - 1)p_2^{e_2-1} \cdots (p_t - 1)p_t^{e_t-1} & \text{si } s \neq 0 \\ (p_1 - 1)p_1^{e_1-1}(p_2 - 1)p_2^{e_2-1} \cdots (p_t - 1)p_t^{e_t-1} & \text{si } s = 0 \end{cases}$$

Empezamos entonces la demostración suponiendo que $\varphi(n) = 2^m$, con $m \in \mathbb{N}$. Si hubiera algún $e_i > 1$, por la fórmula antes vista tendríamos que

$p_i|2^m$. Esto no puede ser, porque p_i es impar y 2^m no puede tener divisores impares. Por tanto, $e_i = 1$, $\forall i = 1, \ldots, t$.

Por tanto, tenemos

$$2^m = (p_i - 1)(p_2 - 1)\cdots(p_t - 1)$$

de donde deducimos directamente que $p_i - 1 = 2^{r_i}$, con $r_i \geq 1$. Así, concluimos que

$$p_i = 2_i^r + 1$$

y que n es de la forma que buscábamos.

Para probar la otra implicación, supongamos que $n = 2^s p_1 \cdots p_t$, con $p_i = 2^{2^{s_i}} + 1$. Por la fórmula de la función totiente, tenemos que

$$\varphi(n) = \begin{cases} 2^{s-1}(p_i - 1)\cdots(p_t - 1) = 2^{a-1}2^{2^{s_1}}2^{2^{s_2}}\cdots 2^{2^{s_t}} & \text{si } s \neq 0 \\ (p_i - 1)\cdots(p_t - 1) = \quad 2^{2^{s_1}}2^{2^{s_2}}\cdots 2^{2^{s_t}} & \text{si } s = 0 \end{cases}$$

En cualquiera de los casos $\varphi(n)$ es una potencia de 2, tal y como buscábamos.

Ejercicio 2. *Para cada entero positivo primo llamamos $\mathcal{P}_{p,n}$ al número de polinomios mónicos irreducibles de grado n sobre $\mathbb{F}_p$.*

Apartado 2.1. Prueba que $p^m = \sum_{j|m} j\mathcal{P}_{p,j}$.

Solución. Llamemos $q = p^m$. El cuerpo de descomposición de $X^q - X$ es $\mathbb{F}_q$. Cada irreducible $P_j(X)$ de grado j descompone en $\mathbb{F}_q$ y cada elemento de $\mathbb{F}_q$ es una raíz de $X^q - X$. Es decir, tenemos que

$$P(X)|X^q - X$$

Además, $P_j(X)$ no tiene raíces múltiples, así que cada irreducible $P_j(X)$ tal que $j|m$ debe aparecer en la factorización una única vez. Por tanto, tenemos la siguiente descomposición:

$$X^q - X = \prod_{j|m} P_j(X)$$

Tomando grados, la igualdad que queríamos demostrar es clara:

$$p^m = q = \sum_{j|m} j\mathcal{P}_{p,j}$$

Apartado 2.2. Si m es primo, prueba que se tiene $\mathcal{P}_{p,m} = \frac{p^m - p}{m}$.

Solución. Sabemos que $\mathbb{F}_{p^m}$ es el cuerpo de descomposición del polinomio $g(X) = X^{p^m} - X$ y que todo polinomio mónico irreducible de grado m divide a g.

Por otro lado, como $|\mathbb{F}_{p^m} : \mathbb{F}_p| = m$, no puede haber subextensiones y, por tanto, todo polinomio irreducible que sea factor de g tiene que tener grado m o 1.

Como cada polinomio lineal sobre $\mathbb{F}_p$ divide a g —dado que para cada $a \in \mathbb{F}_p$, $g(a) = 0$—, y teniendo en cuenta que g tiene todas las raíces simples, concluimos que tenemos p polinomios lineales diferentes que dividen a g.

Igual que antes, tomando grados, la suma de todos los polinomios mónicos irreducibles que dividen a g nos da p^m.

Por tanto, tenemos la relación $m\mathcal{P}_{p,m} + p = p^m$. Despejando, obtenemos la fórmula buscada:

$$\mathcal{P}_{p,m} = \frac{p^m - p}{m}$$

Apartado 2.3. Determina el número de polinomios mónicos irreducibles de grado 3 sobre el cuerpo $\mathbb{F}_3$.

Solución. Podemos usar la fórmula del apartado anterior, de manera que hay

$$\mathcal{P}_{3,3} = \frac{3^3 - 3}{3} = 8$$

polinomios mónicos irreducibles de grado 3 sobre el cuerpo $\mathbb{F}_3$.