Tarea Cuatro.
Teoría de números uno.

Contreras Mendoza Ximena de la Luz

24 de abril de 2020

Ejercicio 1. Pruebe que $d(n)$ es impar si y solo si n es un cuadrado, es decir existe $m \in \mathbb{Z}^+$ tal que $n = m^2$.

Demostración. $\Leftarrow$)
Por hipótesis

$$n = m^2 \tag{1}$$

Consideremos la factorización en potencia de primos de m. Sea $m = p_1^{\beta_1} \cdots p_t^{\beta_t}$ dicha factorizació, sustituyendo en la ecuación (1) tenemos:

$$n = (p_1^{\beta_1} \cdots p_t^{\beta_t})^2 = p_1^{2\beta_1} \cdots p_t^{2\beta_t} \tag{2}$$

Aplicando la función contadora de divisores a la ecuación (2) nos queda

$$d(n) = d(p_1^{2\beta_1} \cdots p_s^{2\beta_s}) \tag{3}$$

Ahora un corolario visto en clase:
Corolario 1.
Si p es primo y $\alpha \geqslant 0$ entonces $d(p^\alpha) = \alpha + 1$. En general si $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ factorización en primos de n entonces $d(n) = d(p_1^{\alpha_1} \cdots p_t^{\alpha_t}) = (\alpha_1 + 1) \cdots (\alpha_t + 1)$.

Aplicando el **Corolario 1**. a la ecuación (3)

$$d(n) = (2\beta_1 + 1) \cdots (2\beta_s + 1) \tag{4}$$

Algunos resultados.

I. El producto de impares es impar:
Prueba.
Sea $2n+1$ con $n \in \mathbb{Z}$ un número impar. Multiplicando $(2n+1)(2m+1) = 4nm+2n+2m+1 = 2(2nm+n+m)+1$. Como $n, m \in \mathbb{Z} \Rightarrow (2nm + n + m) \in \mathbb{Z}$. Sea $k = (2nm + n + m)$ por lo tanto $(2n + 1)(2m + 1) = 2k + 1$ con $k \in \mathbb{Z}$. Así el producto de impares es impar.

II. El producto de pares es par:
Prueba.
Sea $2n$ con $n \in \mathbb{Z}$ un número par. Multiplicando $(2n)(2m) = 4nm = 2(2nm)$. Sea $k = (2nm)$ por lo tanto $(2n)(2m) = 2k$ con $k \in \mathbb{Z}$. Así el producto de pares es par.

III. El producto de un impar con un par, es par:
Prueba.
Multiplicando $(2n+1)(2m) = 4nm+2m = 2(2nm+m)$. Como $n, m \in \mathbb{Z} \Rightarrow (2nm+m) \in \mathbb{Z}$. Sea $k = (2nm+m)$ por lo tanto $(2n + 1)(2m) = 2k$. Así el producto de un impar con un par, es par.

Así en la ecuación (4) para toda i, $2\beta_i + 1$ es un número impar. Como el producto de impares es impar, $d(n) = 2k + 1$ para alguna $k \in \mathbb{Z}$. En particular $2k + 1 > 0$ pues para toda i, $2\beta_i + 1 > 0$.

$\Rightarrow$)
Por hipótesis

$$d(n) = 2k + 1 \tag{5}$$

Sea

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \tag{6}$$

Factorización en potencia de primos de n. Aplicando la función contadora de divisores a la ecuación (6)

$$d(n) = d(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) \tag{7}$$

Aplicando el **Corolario 1**. a la ecuación (7)

$$d(n) = (\alpha_1 + 1) \cdots (\alpha_s + 1) \tag{8}$$

Juntando la ecuación (5) y (8) Obtenemos:

$$2k + 1 = (\alpha_1 + 1) \cdots (\alpha_s + 1) \tag{9}$$

Por los resultados $I.$ $II.$ y $III.$ concluimos que para toda i, $\alpha_i + 1$ debe ser impar, i.e. $\alpha_i + 1 = 2m_i + 1 \Rightarrow \alpha_i = 2m_i \Longrightarrow 2 \mid \alpha_i$ para toda i, entonces $\exists b \in \mathbb{Z}$ tal que $n = b^2$ □

Ejercicio 2. Pruebe que para toda $n > 1$ se tiene:

$$\prod_{d|n} d = n^{\frac{d(n)}{2}}$$

Demostración. Sea $n > 1$. Consideremos el conjunto $D_n := \{d \in \mathbb{Z}^+ : d \mid n\} = \{1 = d_1, d_2, ..., d_t = n\}$.
Como D_n es un conjunto finito de enteros positivos podemos acomodarlos de menor a mayor. Supongamos $1 = d_1 < d_2 < \cdots < d_t = n$. Ahora, para toda $i \in \{1, 2, ..., t\}$, podemos considerar el conjugado de d_i, es decir, si $d_i \in D_n$ entonces la pareja $\{d_i, \frac{n}{d_i}\} \subseteq D_n$. Podemos ver el conjunto D_n como la unión de divisores y sus conjugados. Observemos que $(d_i)\frac{n}{d_i} = n \quad \forall\ i = 1, 2, ..., t$.
Así al hacer el producto de parejas obtenemos

$$(d_1)\frac{n}{d_1} \cdots (d_t)\frac{n}{d_t} = \underbrace{n * n * \cdots * n}_{t\ veces} = n^t \tag{10}$$

Por otro lado al hacer la lista de parejas, podemos ver que se repiten.
1. $\{d_1, \frac{n}{d_1}\} = \{1, \frac{n}{1}\} = \{1, n\}$
2. $\{d_2, \frac{n}{d_2}\}$

$\vdots \qquad \vdots$

t. $\{d_t, \frac{n}{d_t}\} = \{n, \frac{n}{n}\} = \{n, 1\}$

De aquí podemos concluir que nuestra lista de parejas es:
1. $\{d_1, d_t\} = \{1, \frac{n}{1}\} = \{1, n\}$
2. $\{d_2, d_{t-1}\}$

$\vdots \qquad \vdots$

t. $\{d_t, d_1\} = \{n, \frac{n}{n}\} = \{n, 1\}$

Por lo tanto en la ecuación (10) estamos multiplicando de más, estamos multiplicando cada divisor de n dos veces. Es decir nuestra ecuación realmente se ve así:

$$(d_1)^2 \cdots (d_t)^2 = n^t \tag{11}$$

Elevando a la $\frac{1}{2}$ a la ecuación (11) nos queda.

$$(d_1)(d_2) \cdots (d_{t-1})(d_t) = n^{t/2}$$

Así tenemos que el producto de todos los divisores de n es igual a $n^{t/2}$. Como t era el número de divisores de n, es decir $t = d(n)$. Por lo tanto

$$\prod_{d|n} d = n^{\frac{d(n)}{2}}$$

□

Ejercicio 3. Pruebe que $\sigma(1)+\sigma(2)+\ldots+\sigma(n)\leqslant n^2$ para toda $n>1$.

Hint: acomoden los sumandos del lado derecho en un arreglo triangular y cambien el orden de la suma.

$+1$				$\sigma(1)$
$+1$	$+2$			$\sigma(2)$
$+1$		$+3$		$\sigma(3)$
$\vdots$		$\cdots$		$\vdots$
$+1$	$\cdots$		n	$\sigma(n)$
		Total		
$1k_1$	$+2k_2$	$+3k_3$	$\cdots$	$+nk_n$

Demostración. Tenemos que

$$\sigma(1)+\sigma(2)+\ldots+\sigma(n)=1k_1+2k_2+3k_3+\cdots+nk_n \tag{12}$$

Nuestros valores k_i con $i=1,2,...n$ los conocemos. Los obtenemos por el Algoritmo de la división. En efecto, podemos calcularlos fácilmente.

Para $i=1$ tenemos que $n=1n+r$ con $r=0$ así $k_1=n$.
Para $i=2$ tenemos que $n=2b+r$ con $0\leqslant r\leqslant b$ así $b=k_2$.
$\vdots$
Para $i=n$ tenemos que $n=n1+r$ con $r=0$ así $1=k_n$.

Que pasaría si esto no fuera así. Sea $j\in\{1,2,...,n\}$ entonces $n=jz+r$ con $z\in\mathbb{Z}$ y $0\leqslant r\leqslant z$. Si k_j fuera distinto de z entonces se cumplen dos casos.
1) $k_j<z$
Entonces debe existir al menos un valor $x\in\{1,2,...,n\}$ tal que $j\mid x$ pero estoy sumando $\sigma(x)-j$ ó no estoy sumando $\sigma(x)$ por lo tanto mi suma es erronea.
2) $k_j>z$
Entonces estoy contando de más. Es decir tengo un valor $m>n$ tal que $j\mid m$ entonces mi suma queda $\sigma(1)+\sigma(2)\ldots+\sigma(n)+\sigma(m)$ por lo tanto mi suma es erronea.

Por lo tanto utilizando el algoritmo de la división encontramos k_i con $i=1,2,...,n$. Observemos que $n=k_1>k_2\geqslant ...\geqslant k_n=1$. En efecto, si $a<\alpha$ entonces

$$n=ab+r\quad p.a.\quad b\in\mathbb{Z},\ 0\leqslant r\leqslant b$$

Por otro lado

$$n=\alpha\beta+t\quad p.a.\quad \beta\in\mathbb{Z},\ 0\leqslant t\leqslant b$$

Como $a<\alpha$ debe suceder que $\beta\geqslant b$.

Por lo tanto en la ecuación (12) tenemos una suma, de n sumandos, donde cada sumando es menor o igual a n. Por lo tanto

$$\sigma(1)+\sigma(2)+\ldots+\sigma(n)\leqslant \underbrace{n+n+...+n}_{n\ veces}=n^2$$

Para toda $n>1$ □

Ejercicio 4. Pruebe que $\varphi(n)$ es par, para toda $n>1$.

Demostración. Observemos que n debe ser mayor que 2 pues $\varphi(2)=1$, que es impar.

Consideremos la factorización en potencia de primos de n, ecuación (6). Por otro lado, sabemos que φ es una función multiplicativa. Es decir, la función φ cumple que si $(a,b)=1$ entonces $\varphi(ab)=\varphi(a)\varphi(b)$.
Tenemos que $(p_1,p_2,...,p_s)=1$, pues son primos distintos dos a dos, entonces $(p_1^{\alpha_1},p_2^{\alpha_2},...,p_s^{\alpha_s})=1$. Aplicando φ a la ecuación (6) obtenemos:

$$\varphi(n)=\varphi(p_1^{\alpha_1}\cdots p_s^{\alpha_s})=\varphi(p_1^{\alpha_1})\cdots\varphi(p_s^{\alpha_s})=(p_1-1)p_1^{\alpha_1-1}\cdots(p_s-1)p_s^{\alpha_s-1} \tag{13}$$

Afirmación 1.
Todo $p\in\mathbb{P}$ tal que $p\neq 2$ cumple que $p-1$ es par.
Prueba.
Sea $p\in\mathbb{P}$ con $p\neq 2$ supongamos que $p-1$ no es par, entonces $p-1=2m+1\Rightarrow p=2m+2=2(m+1)\Rightarrow 2\mid p$ $\quad\rightarrow\leftarrow$ pues p, es primo distinto de dos.

Así la ecuación (13) cumple que $\forall i, \quad p_i - 1$ es par, excepto cuando $p_j = 2$. Utilizando la parte de **Algunos resultados** en el **Ejercicio 1.** más específicamente $II.$ y $III.$ concluimos $\varphi(n)$ es par. □

Ejercicio 5. Pruebe que para todo $n > 1$ se tiene que

$$\sum_{k=1 \ (n,k)=1}^{n} k = \frac{n}{2}\varphi(n)$$

donde la suma corre sobre el conjunto $\{1 \leqslant k \leqslant n : (n,k) = 1\}$

Hint: prueba que $(n,k) = 1 \iff (n, n-k) = 1$, de esta manera los elementos en $\{1 \leqslant k \leqslant n : (n,k) = 1\}$ vienen en parejas de la forma $(k, n-k)$

Demostración. Sea $\mathbb{A} = \{1 \leqslant k \leqslant n : (n,k) = 1\} = \{k_1, k_2, ..., k_m\}$ con $m = \varphi(n)$.

Observación 1.
$\mathbb{A}$ es un conjunto finito de enteros.

Como $(n,k) = 1 \iff (n, n-k) = 1$ para cada k_i tengo que $n - k_i \in \mathbb{A}$, es decir
$\mathbb{A} = \{1 \leqslant k \leqslant n : (n, n-k) = 1\}$. Por la **Observación 1.** entonces debe $\exists j \in \{1, ..., m\}$ tal que $k_i = n - k_j$ para toda $i \in \{1, ..., m\}$. Pongámoslos en parejas:

$$\begin{matrix} k_1 & k_m \\ \vdots & \vdots \\ k_m & k_1 \end{matrix} \quad \Longrightarrow \quad \begin{matrix} k_1 & n-k_1 \\ \vdots & \vdots \\ k_m & n-k_m \end{matrix}$$

Sumémoslos:

$$\begin{aligned}(k_1 + k_2 + ... + k_m) + (n-k_1) + (n-k_2) + ... + (n-k_m) &= k_1 + (n-k_1) + k_2 + (n-k_2) + ... + k_m + (n-k_m) \\ &= \underbrace{n + n + ... + n}_{m=\varphi(n) veces} \\ &= n\varphi(n)\end{aligned}$$

Por lo tanto

$$(k_1 + k_2 + ... + k_m) + (n-k_1) + (n-k_2) + ... + (n-k_m) = n\varphi(n) \tag{14}$$

Por otro lado:

$$\begin{aligned}(k_1 + k_2 + ... + k_m) + (n-k_1) + (n-k_2) + ... + (n-k_m) &= k_1 + (n-k_m) + ... + k_m + (n-k_1) \\ &= 2k_1 + ... + 2k_m \\ &= 2(k_1 + ... + k_m)\end{aligned}$$

Por lo tanto

$$(k_1 + ... + k_m) + (n-k_1) + ... + (n-k_m) = 2(k_1 + ... + k_m) \tag{15}$$

Juntando las ecuaciones (14) y (15) tenemos que:

$$2\sum_{k=1}^{n} k = n\varphi(n) \quad \Longrightarrow \quad \sum_{k=1}^{n} k = \frac{n}{2}\varphi(n)$$

Bastaría solo probar el Hint. $(n,k) = 1 \iff (n, n-k) = 1$
Prueba.
$\Rightarrow$)
Por hipótesis $(n,k) = 1 \Longrightarrow \exists a, b \in \mathbb{Z}$ tal que

$$an + bk = 1 \tag{16}$$

De la ecuación (16) tenemos que:

$$1 = an + (bn - bn) + bk = (a+b)n + (-b)(n-k)$$

Por lo tanto

$$(a+b)n - b(n-k) = 1 \tag{17}$$

Con $-b, a+b \in \mathbb{Z}$. Por lo tanto $(n, n-k) = 1$

$\Leftarrow$)
Por hipótesis $(n, n-k) = 1$ entonces, tenemos que se cumple la ecuación (17). Como nuestra ecuación (17) implica la ecuación (16) que implica que $(n,k) = 1$. Tenemos que si $(n, n-k) = 1 \Rightarrow (n,k) = 1$ □