El Teorema Fundamental de la Aritmética

Por Carlos Jacob Rubio Barrios

Nivel Intermedio

Cuando un número entero a se divide por un número entero b y se obtiene residuo cero, es decir, $a = bq$ para algún entero q, decimos que b es un divisor de a o que b divide a, y se denota por $b \mid a$. Así por ejemplo, 4 y 5 son divisores de 20. Al número 20 podemos encontrarle otros números que tienen la misma propiedad que el 5 o el 4; todos serían sus *divisores*. En concreto, $1, 2, 4, 5, 10, 20$ son todos los divisores positivos de 20. Sin embargo, existen números cuyos divisores positivos son sólo dos: el mismo número y el 1. A estos números los denominamos *números primos*. Así pues, $2, 3, 5, 7, 11, 13$ son los ejemplos más sencillos de números primos. El número 1 no se considera primo por razones que veremos más adelante. Un número entero n que no es primo, es decir, que tiene un divisor a tal que $1 < a < n$, se llama *compuesto*.

Los números primos son los ladrillos con los que se construye el edificio de todos los números. Todo número se puede escribir como producto de números primos y esta manera de escribirlo es única. Por ejemplo, 30 se puede escribir como producto de 2, 3 y 5. Este resultado sobre la factorización de un número como producto de números primos era conocido ya por los griegos y hoy día se conoce como el *Teorema Fundamental de la Aritmética (TFA)* por su importancia.

Los números primos poseen una propiedad muy especial que, en general, no poseen los números compuestos, a saber, si p es un número primo y a y b son enteros tales que $p \mid ab$, entonces $p \mid a$ o $p \mid b$. La demostración de esta propiedad no la daremos aquí, y la dejaremos para un futuro artículo, aunque usaremos la propiedad en la demostración del TFA. Sin embargo, veamos que cuando p no es primo, en general no se cumple dicha propiedad. Consideremos el número 6 que no es primo. Observemos que 6 divide

a $8 \cdot 9$ y sin embargo, 6 no divide ni a 8 ni a 9.

Comenzaremos demostrando un resultado que será útil a lo largo de todo el texto.

Proposición 1 *Todo entero $n > 1$ tiene un divisor primo.*

Demostración. Si n es primo, entonces n es un divisor primo de n. Supongamos que n no es primo y sea a su divisor más pequeño mayor que 1. Si a no es primo, entonces $a = a_1 a_2$ con $1 < a_1 \leq a_2 < a$. Como $a_1 \mid a$ y $a \mid n$, tenemos que $a_1 \mid n$. Luego, a_1 es un divisor de n menor que a y mayor que 1, lo cual contradice la elección de a. Por lo tanto, a es un divisor primo de n. □

Los números primos han suscitado a lo largo de la historia la curiosidad de los matemáticos, tanto profesionales como aficionados. Ya Euclides en el año 300 a.C. (en la proposición 20 del libro IX de los *Elementos*), demostró que hay una infinidad de números primos. A continuación damos la demostración de este hecho debida a Euclides.

Proposición 2 *Hay una infinidad de números primos.*

Demostración. Supongamos, por contradicción, que hay sólo un número finito de números primos, digamos $p_1, p_2, \ldots, p_k$. Consideremos el número $N = p_1 p_2 \cdots p_k + 1$. Por la Proposición 1 sabemos que N tiene un divisor primo q. Luego, q debe ser uno de los números primos de la lista. Entonces, q divide al producto $p_1 p_2 \cdots p_k$ y a N. Por lo tanto, q divide también a la diferencia $N - p_1 p_2 \cdots p_k$ que es igual a 1, lo cual no es posible. Por lo tanto, hay una infinidad de números primos. □

Un problema interesante es preguntarse si un número aleatorio es primo o no. Para saberlo, lo más sencillo es empezar a dividir el número por los primos más pequeños. Comenzamos por el 2 y si la división da residuo 0 sabemos que no puede ser primo. En caso contrario, probamos con el 3: si la división da residuo 0 no es primo, en caso contrario, probamos con el 5. Podemos continuar de esta forma con todos los números primos más pequeños que el número; si ninguna de las divisiones anteriores da residuo 0 podemos afirmar que el número que estábamos probando es primo. Realmente no hay que probar con todos los números primos más pequeños que nuestro número; podemos quedarnos con los que sean menores o iguales que la raíz cuadrada del número como se demuestra en el siguiente resultado.

Proposición 3 *Si $n > 1$ es un número compuesto, entonces n tiene un divisor primo p tal que $p \leq \sqrt{n}$.*

Demostración. Sea $n > 1$ un número compuesto. Entonces, n tiene un divisor d tal que $1 < d < n$. Escribamos $n = dd'$ con d' un entero. Observemos que $1 < d' < n$, pues si $d' = 1$ entonces $n = d$ que es una contradicción, y si $d' = n$, entonces $d = 1$ que es una contradicción. Si $d > \sqrt{n}$ y $d' > \sqrt{n}$, entonces $n = dd' > \sqrt{n}\sqrt{n} = n$, lo que es una contradicción. Por lo tanto, $d \leq \sqrt{n}$ o $d' \leq \sqrt{n}$. Supongamos que $d \leq \sqrt{n}$. Aplicando la Proposición 1, se sigue que d tiene un divisor primo $p \leq d \leq \sqrt{n}$. Luego, p es también un divisor primo de n y $p \leq \sqrt{n}$. El otro caso es análogo. □

A manera de ejemplo, supongamos que queremos determinar si el número 2011 es primo. De acuerdo con la proposición anterior, 2011 será primo si no es divisible entre

ningún primo menor o igual que $\sqrt{2011}$. Como $44 < \sqrt{2011} < 45$, los números primos menores o iguales que 44 son: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41$ y 43. Haciendo las divisiones de 2011 entre cada uno de estos números primos, podemos darnos cuenta que ninguna división da residuo 0 y por lo tanto, concluimos que 2011 es un número primo.

Estamos listos para enunciar y demostrar el TFA.

Teorema 4 (TFA) *Todo entero $n > 1$ es primo o se puede escribir como un producto de números primos. Además, esta factorización como producto de primos es única, es decir, si $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, donde los p_i y los q_i son primos, entonces $r = s$ y los primos p_i son los primos q_i en algún orden.*

Demostración. Sea $n > 1$ un entero compuesto, es decir, no primo. De acuerdo con la Proposición 1, n tiene un divisor primo q_1. Entonces, $n = q_1 q_2$ con q_2 entero tal que $1 < q_2 < n$. Si q_2 es primo, entonces n es producto de números primos. Si q_2 no es primo, entonces nuevamente por la Proposición 1, q_2 tiene un divisor primo q_3. Entonces, $q_2 = q_3 q_4$ con q_3 primo y $1 < q_4 < q_2$, de donde $n = q_1 q_3 q_4$. Si q_4 es primo, entonces n es producto de primos. Si q_4 no es primo, entonces por la Proposición 1, q_4 tiene un divisor primo q_5. Luego, $q_4 = q_5 q_6$ con q_5 primo y $1 < q_6 < q_4 < q_2$, de donde $n = q_1 q_3 q_5 q_6$. Si q_6 es primo, entonces n es producto de primos. Si q_6 no es primo, continuamos el proceso. Como hay un número finito de enteros entre 1 y q_2, el proceso no puede continuar de forma indefinida, de modo que en un número finito de pasos obtendremos que $n = q_1 q_3 q_5 \cdots q_r$ con $q_1, q_3, \ldots, q_r$ números primos.
Para la unicidad de la factorización, supongamos que existe un entero $n > 1$ con dos factorizaciones distintas, y consideremos al menor de dichos enteros (cualquier entero menor que n y mayor que 1, tiene factorización única), digamos,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

donde $p_1, \ldots, p_r, q_1, \ldots, q_s$ son números primos. Es claro que $r \geq 2$ y $s \geq 2$. Demostraremos que $p_i \neq q_j$ para cada $i = 1, 2, \ldots, r$ y cada $j = 1, 2, \ldots, s$. Supongamos, por contradicción, que $p_i = q_j$ para algunos i, j. Podemos suponer que $p_1 = q_1$ ya que el orden de los factores no importa. Tenemos que $n > p_1$ (pues si $n = p_1$, entonces $n = q_1$ y n tendría factorización única). Entonces $1 < \frac{n}{p_1} < n$, de modo que $\frac{n}{p_1}$ tiene factorización única como producto de primos. Como,

$$\frac{n}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s,$$

tenemos que $r = s$ y $p_i = q_i$ para todo $i = 2, \ldots, r$. Esto implica que n tiene factorización única, lo que es una contradicción. Por lo tanto $p_i \neq q_j$ para cada $i = 1, \ldots, r$ y cada $j = 1, \ldots, s$.
Ahora, como p_1 divide al producto $q_1 q_2 \cdots q_s$, tenemos que $p_1 \mid q_j$ para algún j. Luego $p_1 = q_j$, lo cual es una contradicción. Por lo tanto, la factorización de n como producto de primos es única. □

El hecho de que el número 1 no se considere primo, es una convención. Sin embargo, esta convención es necesaria para que se tenga la unicidad en el TFA. Si permitiéramos

que el número 1 sea primo, entonces $6 = 2\cdot 3 = 1\cdot 2\cdot 3 = 1\cdot 1\cdot 2\cdot 3$ serían factorizaciones distintas de 6 como producto de números primos.

Dado un entero $n > 1$ compuesto, podemos escribir su factorización en producto de primos en la forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ donde los primos p_i son tales que $p_1 < p_2 < \cdots < p_r$ y $\alpha_1, \alpha_2, \ldots, \alpha_r$ son enteros positivos. Esta expresión de n recibe el nombre de *factorización canónica*. Por ejemplo, $36 = 2^2 \cdot 3^2$, $92 = 2^2 \cdot 23$, $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, $125 = 5^3$.

A continuación veremos algunas aplicaciones del TFA en la solución de problemas.

Ejemplo 1. Sean a y b enteros positivos primos relativos. Demostrar que si ab es un cuadrado, entonces a y b también son cuadrados.

Solución. Por hipótesis, existe un entero positivo n tal que $ab = n^2$. Consideremos las descomposiciones canónicas de a y b,

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s},$$

donde los primos p_i son distintos entre sí, así como los primos q_j. Entonces,

$$ab = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}.$$

Como a y b son primos relativos, tenemos que $p_i \neq q_j$ para cada $i = 1, \ldots, r$ y cada $j = 1, \ldots, s$, lo que implica que $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \cdot q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ es la factorización canónica de n^2. Como los primos que dividen a n^2 son los mismos primos que dividen a n (si p es primo, entonces $p \mid n^2$ si y sólo si $p \mid n$), el TFA implica que los exponentes que aparecen en la factorización canónica de n^2 son enteros pares, es decir, $\alpha_i = 2\alpha_i'$ para cada $i = 1, \ldots, r$ y $\beta_j = 2\beta_j'$ para cada $j = 1, \ldots, s$. De aquí se sigue que a y b son ambos cuadrados de enteros.

Ejemplo 2. Sean a, b y c enteros positivos. Demostrar que si ab, ac y bc son cubos de enteros, entonces a, b y c también son cubos de enteros.

Solución. Escribamos las factorizaciones en primos de a, b y c, de la siguiente manera:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}, \quad c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r},$$

donde los primos p_i son distintos y los exponentes de cada factorización son enteros mayores o iguales que 0 (observemos que al permitir exponentes iguales a cero, puede haber primos que dividan a alguno de los tres números pero a cualquiera de los otros dos no).
Como $ab = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_r^{\alpha_r+\beta_r}$ es el cubo de un entero, tenemos por el TFA que $ab = (p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})^3$ donde los exponentes son mayores o iguales que cero, de donde $\alpha_i + \beta_i = 3k_i$ para cada $i = 1, \ldots, r$. De manera análoga, como ac y bc son cubos de enteros, tenemos que $\alpha_i + \gamma_i = 3l_i$ para cada $i = 1, \ldots, r$, y $\beta_i + \gamma_i = 3m_i$ para cada $i = 1, \ldots, r$. Resolviendo el sistema de ecuaciones,

$$\alpha_i + \beta_i = 3k_i, \quad \alpha_i + \gamma_i = 3l_i, \quad \beta_i + \gamma_i = 3m_i,$$

obtenemos que $2\beta_i = 3(k_i - l_i + m_i)$ de donde 2 divide a $k_i - l_i + m_i$ ya que 2 y 3 son primos relativos. De aquí se sigue que β_i es múltiplo de 3, y por lo tanto $\alpha_i = 3k_i - \beta_i$

y $\gamma_i = 3m_i - \beta_i$ también son múltiplos de 3 para cada $i = 1, \ldots, r$. Luego, a, b y c son cubos de enteros.

Ejemplo 3. Sean a, b, r, s enteros positivos. Si a y b son primos relativos y $r^a = s^b$, demostrar que existe un entero n tal que $r = n^b$ y $s = n^a$.

Solución. Como $r^a = s^b$, el TFA implica que los números primos que dividen a r son los mismos primos que dividen a s. Supongamos que éstos son $p_1, p_2, \ldots, p_k$. Sea p cualquiera de estos números primos, y supongamos que p^α es la mayor potencia de p que divide a r y p^β es la mayor potencia de p que divide a s. Entonces,

$$r^a = s^b \Rightarrow p^{\alpha a} = p^{\beta b} \Rightarrow \alpha a = \beta b.$$

De aquí, $a \mid \beta b$ y $b \mid \alpha a$. Como a y b son primos relativos, tenemos que $a \mid \beta$ y $b \mid \alpha$. Escribamos $\beta = a\beta_p$ y $\alpha = b\alpha_p$. Entonces, $\alpha a = \beta b \Rightarrow ab\alpha_p = ab\beta_p \Rightarrow \alpha_p = \beta_p$. Ahora, para cada primo p_i que divide a r (y por lo tanto a s), consideremos el entero α_{p_i}. Finalmente, es fácil ver que el número $n = p_1^{\alpha_{p_1}} p_2^{\alpha_{p_2}} \cdots p_k^{\alpha_{p_k}}$ satisface las condiciones del problema.

Ejemplo 4. Sean a, b, c y d enteros positivos tales que $a^3 = b^2$, $c^3 = d^2$ y $a - c = 25$. Determinar los valores de a, b, c y d.

Solución. Como 2 y 3 son primos relativos, podemos aplicar el ejemplo anterior a las igualdades $a^3 = b^2$ y $c^3 = d^2$. Así, existen enteros positivos n y m tales que $a = n^2$, $b = n^3$, $c = m^2$ y $d = m^3$. Luego, $25 = a - c = n^2 - m^2 = (n + m)(n - m)$ de donde la única posibilidad es $n + m = 25$ y $n - m = 1$. De aquí obtenemos que $n = 13$ y $m = 12$. Por lo tanto, $a = 13^2$, $b = 13^3$, $c = 12^2$ y $d = 12^3$.

Ejemplo 5. Determinar todas las parejas de enteros positivos (m, n) con $m \neq n$ que satisfacen la ecuación $m^n = n^m$.

Solución. Supongamos, sin pérdida de generalidad, que $m < n$. La igualdad $m^n = n^m$ junto con el TFA, nos dicen que los divisores primos de m son los mismos divisores primos de n. Escribamos las factorizaciones canónicas de m y n,

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

donde los primos p_i son distintos entre sí, y los exponentes α_i y β_i son enteros positivos. Luego, $(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})^n = (p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k})^m$, de donde $\alpha_i n = m\beta_i$ para cada $i = 1, \ldots, k$. Como $m < n$, necesariamente $\alpha_i \leq \beta_i$ para cada $i = 1, 2, \ldots, k$, lo que significa que $m \mid n$. Escribamos $n = mr$ con $r \geq 2$ (pues $r = 1$ implica que $m = n$ lo cual no puede ser). La ecuación $m^n = n^m$ es equivalente con la ecuación $m^{mr} = (mr)^m$, es decir, $m^{m(r-1)} = r^m$.
Si $r = 2$, entonces $m^m = 2^m$, de donde $m = 2$ y por lo tanto $n = mr = 4$. Así, tenemos la solución $(2, 4)$.
Supongamos que $r \geq 3$. Es claro que $m^{m(r-1)} < r^m$ si $m = 1$. Es un ejercicio fácil demostrar que $2^{r-1} > r$ si $r \geq 3$. Usaremos esta desigualdad para demostrar que $m^{m(r-1)} > r^m$ si $m \geq 2$. Si $m = 2$, tenemos que $2^{2(r-1)} = (2^{r-1})^2 > r^2$. Supongamos que $m^{m(r-1)} > r^m$ para algún $m \geq 2$. Entonces,

$$(m+1)^{(m+1)(r-1)} > m^{(m+1)(r-1)} = m^{m(r-1)} m^{r-1} > r^m \cdot 2^{r-1} > r^m \cdot r = r^{m+1}.$$

Por lo tanto, si $r \geq 3$ la ecuación no tiene soluciones.
Concluimos que la única solución (m, n) con $m < n$ es $(2, 4)$, y por la simetría de la ecuación, la única solución (m, n) con $m > n$ es $(4, 2)$.

Algunas consecuencias del TFA

Una vez que sabemos que es posible factorizar todo número entero en producto de números primos, una pregunta natural que surge es: ¿cómo son los divisores de un número entero en términos de sus divisores primos? Esta y otras preguntas las responderemos a continuación.

Teorema 5 *Si $n > 1$ es un entero y $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ es su factorización canónica en producto de primos distintos, entonces cada divisor positivo de n es de la forma $p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ donde $0 \leq \beta_i \leq \alpha_i$ para cada $i = 1, \ldots, k$.*

Demostración. Observemos primero que si $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ con $0 \leq \beta_i \leq \alpha_i$ para cada $i = 1, \ldots, k$, entonces $d \mid n$, pues $n = d(p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \cdots p_k^{\alpha_k - \beta_k})$ con $\alpha_i - \beta_i \geq 0$ para cada $i = 1, \ldots, k$. Ahora debemos demostrar que n no tiene otros divisores distintos de d. Claramente $1 = p_1^0 p_2^0 \cdots p_k^0$. Supongamos que $d' > 1$ es un divisor de n y sea p un divisor primo de d' (tal primo existe por la Proposición 1). Sea p^γ la mayor potencia de p que divide a d', es decir, $d' = p^\gamma k$ donde $p \nmid k$. Como d' es divisor de n, tenemos que p^γ también es divisor de n. Por la unicidad de la factorización en primos del número n, se sigue que $p = p_j$ para algún $1 \leq j \leq k$ y $\gamma \leq \alpha_j$. Así, $d' = p_j^\gamma k$ con $p_j \nmid k$ y $\gamma \leq \alpha_j$. Si $k = 1$, terminamos. Supongamos que $k > 1$. Por la Proposición 1, k tiene un divisor primo q. Como $p \nmid k$, tenemos que $q \neq p$. Sea q^δ la mayor potencia de q que divide a k, esto es, $k = q^\delta k'$ donde $q \nmid k'$. Entonces, q^δ divide a n y nuevamente por la unicidad de la factorización en primos del número n tenemos que $q = p_l$ para algún $l \neq j$ y $\delta \leq \alpha_l$. Así, $d' = p_j^\gamma p_l^\delta k'$ donde $p_j \nmid k'$, $p_l \nmid k'$, $\gamma \leq \alpha_j$ y $\delta \leq \alpha_l$. Continuando de esta manera, obtenemos que $d' = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ donde $0 \leq \beta_i \leq \alpha_i$ para cada $i = 1, \ldots, k$. □

Hemos demostrado así que d es un divisor positivo de n si y sólo si $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ con $0 \leq \beta_i \leq \alpha_i$ para cada $i = 1, \ldots, k$. Podemos preguntarnos ahora: ¿cuántos números de esta forma hay?
Como cada β_i puede tomar $\alpha_i + 1$ valores (desde 0 hasta α_i), por el principio del producto tenemos $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ divisores positivos distintos de n. Usualmente se denota por $\tau(n)$ al número de divisores positivos de n.
Si m y n son enteros positivos primos relativos, es fácil ver que $\tau(mn) = \tau(m)\tau(n)$, pues los divisores primos de m son distintos de los divisores primos de n.

También podemos preguntarnos por la suma de los divisores positivos de un entero positivo n. Esta suma usualmente se denota por $\sigma(n)$ y matemáticamente representa la suma $\sum_{d|n} d$, la cual se efectúa sobre los divisores positivos d de n. Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, entonces por el Teorema 5 tenemos que $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ donde

$0 \leq \beta_i \leq \alpha_i$ para cada $i = 1, \ldots, k$. Luego, tenemos que,

$$\begin{aligned}\sigma(n) &= \sum_{d|n} d = \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \cdots \sum_{\beta_k=0}^{\alpha_k} p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \\ &= \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1} \right) \left(\sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2} \right) \cdots \left(\sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k} \right).\end{aligned}$$

Por lo tanto, basta calcular $\sum_{\beta_i=0}^{\alpha_i} p_i^{\beta_i} = 1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}$. Usando la fórmula $\sum_{i=0}^{n} x^i = \frac{x^{n+1}-1}{x-1}$ válida si $x \neq 1$, obtenemos que $\sum_{\beta_i=0}^{\alpha_i} p_i^{\beta_i} = \frac{p^{\alpha_i+1}-1}{p_i-1}$, y por lo tanto,

$$\sigma(n) = \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1} \right) \left(\frac{p_2^{\alpha_2+1}-1}{p_2-1} \right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k-1} \right).$$

Es fácil ver que $\sigma(mn) = \sigma(m)\sigma(n)$ si m y n son enteros positivos primos relativos.

Veamos algunos ejemplos.

Ejemplo 6. Sea n un entero positivo. Demostrar que $\tau(n) \leq 2\sqrt{n}$.

Solución. Sea d un divisor positivo de n. Es claro que $d \mid n$ si y sólo si $\frac{n}{d} \mid n$. Supongamos que n tiene k divisores positivos menores o iguales que $\sqrt{n}$. Claramente $k \leq \sqrt{n}$. Luego, por cada divisor positivo d menor o igual que $\sqrt{n}$ hay un divisor positivo mayor o igual que $\sqrt{n}$, a saber, $\frac{n}{d}$. De aquí que n tiene a lo más k divisores positivos mayores o iguales que $\sqrt{n}$ (si n es un cuadrado, el número de divisores positivos mayores o iguales que $\sqrt{n}$ es $k-1$). Por lo tanto, $\tau(n) \leq 2k \leq 2\sqrt{n}$.

Ejemplo 7. Un entero positivo es llamado *solitario* si la suma de los recíprocos de sus divisores positivos no es igual a la suma de los recíprocos de los divisores positivos de cualquier otro entero positivo. Demostrar que todo número primo es solitario.

Solución. Denotemos por $\sigma_{-1}(n)$ a la suma de los recíprocos de los divisores positivos de n, es decir, $\sigma_{-1}(n) = \sum_{d|n} \frac{1}{d}$. Luego,

$$\sigma_{-1}(n) = \sum_{d|n} \frac{1}{d} = \frac{1}{n} \sum_{d|n} \frac{n}{d} = \frac{1}{n} \sum_{d'|n} d' = \frac{1}{n}\sigma(n), \tag{1}$$

donde la igualdad $\sum_{d|n} \frac{n}{d} = \sum_{d'|n} d'$ se sigue de que $d \mid n$ si y sólo si $\frac{n}{d} \mid n$.
Si $p \geq 2$ es primo, entonces $\sigma_{-1}(p) = 1 + \frac{1}{p} = \frac{p+1}{p}$. Supongamos que p no es solitario, es decir, supongamos que existe un entero positivo $n \neq p$ tal que $\sigma_{-1}(n) = \frac{p+1}{p}$. Aplicando la relación (1), tenemos que $\frac{1}{n}\sigma(n) = \frac{p+1}{p}$, de donde $p\sigma(n) = n(p+1)$. Como p es primo relativo con $p+1$, tenemos que $p \mid n$ y como $n \neq p$, se sigue que,

$$\sigma_{-1}(n) = \sum_{d|n} \frac{1}{d} \geq 1 + \frac{1}{p} + \frac{1}{n} > \sigma_{-1}(p),$$

lo cual es una contradicción. Por lo tanto, todo número primo es solitario.

Ejemplo 8. Determinar todos los enteros positivos n que tienen exactamente 16 divisores positivos $d_1, d_2, \ldots, d_{16}$, tales que $1 = d_1 < d_2 < \cdots < d_{16} = n$, $d_6 = 18$ y $d_9 - d_8 = 17$.

Solución. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ la factorización canónica de n. Entonces, n tiene $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$ divisores positivos. Luego, $18 = 2 \cdot 3^2$ tiene 6 divisores positivos: $1, 2, 3, 6, 9$ y 18. Como n tiene 16 divisores positivos, tenemos que $n = 2 \cdot 3^3 p$ para algún primo p o $n = 2 \cdot 3^7$. Si $n = 2 \cdot 3^7$, entonces $d_8 = 54$, $d_9 = 81$ y $d_9 - d_8 \neq 17$, lo cual es una contradicción. Luego, $n = 2 \cdot 3^3 p$ para algún primo $p > 18$. Si $p < 27$, entonces $d_7 = p$, $d_8 = 27$, $d_9 = 2p = 27 + 17 = 44 \Rightarrow p = 22$, lo cual es una contradicción. Por lo tanto, $p > 27$. Si $p < 54$, entonces $d_7 = 27$, $d_8 = p$, $d_9 = 54 = d_8 + 17 \Rightarrow p = 37$. Si $p > 54$, entonces $d_7 = 27$, $d_8 = 54$, $d_9 = d_8 + 17 = 71$. Así, tenemos dos posibles soluciones: $2 \cdot 3^3 \cdot 37 = 1998$ y $2 \cdot 3^3 \cdot 71 = 3834$.

Ejemplo 9. Determinar todos los enteros positivos n tales que $\tau(n) = \frac{n}{3}$.

Solución. Sea n un entero positivo que satisface la condición $\tau(n) = \frac{n}{3}$. Entonces, $3 \mid n$. Escribamos $n = 3k$, con k entero positivo.
Si k es par, entonces $\frac{k}{2} = \frac{n}{6}$ es un divisor de n. Más aún, si todos los enteros positivos menores que $\frac{n}{6}$ son divisores de n y los números $\frac{n}{5}, \frac{n}{4}, \ldots, \frac{n}{1}$ son también divisores de n, tenemos que $\frac{n}{3} = \tau(n) \leq \frac{n}{6} + 5$, de donde $n \leq 30$. Luego, los posibles valores de n son: $6, 12, 18, 24$ y 30. De estos, es fácil ver que sólo 18 y 24 satisfacen la condición del problema.
Si $k = \tau(n)$ es impar, entonces n es un cuadrado según el Ejercicio 5. Supongamos que $n = m^2$. Como k es impar, $n = 3k$ también es impar, de modo que m es impar. De acuerdo al Ejemplo 6 tenemos que $\frac{m^2}{3} = \tau(m^2) \leq 2m$ de donde $m \leq 6$. Como m es impar, los valores posibles de m son $1, 3$ y 5, y en consecuencia $n = 1, 9$ o 25. Como n es múltiplo de 3, el único número que cumple es 9.
Por lo tanto, el problema admite tres soluciones: 9, 18 y 24.

Solución alternativa. Como $3 \mid n$, se sigue que la factorización canónica de n es de la forma $n = 3^{\alpha} \cdot p_1^{\alpha_1} \cdots p_j^{\alpha_j}$, de donde $\tau(n) = (\alpha+1)(\alpha_1+1)\cdots(\alpha_j+1)$. La condición $\tau(n) = \frac{n}{3}$ implica que $3^{\alpha-1} \cdot p_1^{\alpha_1} \cdots p_j^{\alpha_j} = (\alpha+1)(\alpha_1+1)\cdots(\alpha_j+1)$. Como $p_i^{\alpha_i} \geq 2^{\alpha_1} \geq \alpha_i + 1$, para que n satisfaga la ecuación del problema, es necesario que $\alpha + 1 \geq 3^{\alpha-1}$, de donde $\alpha = 1$ o $\alpha = 2$.
Si en la factorización de n hay un primo $p_i > 3$, entonces $p_i^{\alpha_i} > 4^{\alpha_i} \geq 2\alpha_i + 2$ y la igualdad $\tau(n) = \frac{n}{3}$ no se daría. Por lo tanto, n no tiene divisores primos mayores que 3. Si $\alpha = 1$, entonces $n = 3 \cdot 2^m$ y la igualdad $\tau(n) = \frac{n}{3}$ se reduce a $2(m+1) = 2^m$. Es fácil ver que $m = 1$ o 2 no cumplen; $m = 3$ es solución y por lo tanto $n = 24$. Si $m \geq 4$ tampoco hay soluciones ya que $2^m > 2m + 2$. De manera análoga, si $\alpha = 2$, entonces $n = 3^2 \cdot 2^m$ y la igualdad $\tau(n) = \frac{n}{3}$ se reduce a $3(m+1) = 3 \cdot 2^m$ cuyas únicas soluciones son $m = 0$, 1, y por lo tanto, $n = 9$, 18.

Ejemplo 10. Demostrar que hay una infinidad de enteros positivos n tales que $\frac{\sigma(2^n-1)}{n}$ es un entero.

Solución. Demostraremos que todos los enteros positivos de la forma $n = 2^k$ satisfacen el problema. Lo haremos por inducción en k. Si $k = 0$, tenemos que $n = 1$ y $\frac{\sigma(2^1-1)}{1} = 1$. Supongamos que el resultado es cierto para $n = 2^k$ con $k > 0$, y consideremos el número $2n = 2^{k+1}$. Entonces, $2^{2n} - 1 = (2^n)^2 - 1 = (2^n + 1)(2^n - 1)$. Como $2^n + 1$ y $2^n - 1$ son primos relativos (si d es un divisor de $2^n + 1$ y $2^n - 1$, entonces d debe dividir a su diferencia que es igual a 2, de donde $d = 1$ o 2, y como ambos números son impares, su único divisor común es 1), tenemos que $\sigma(2^{2n} - 1) = \sigma(2^n + 1)\sigma(2^n - 1)$. Aplicando la hipótesis de inducción, se sigue que $\sigma(2^n - 1)$ es múltiplo de n. Luego, basta demostrar que $\sigma(2^n + 1)$ es par. Como n es par, tenemos que 2^n es un cuadrado y por lo tanto $2^n + 1$ no puede ser un cuadrado (pues $n > 0$). Ahora, por el Ejercicio 6 tenemos que $\sigma(2^n + 1)$ es par y por lo tanto, $\sigma(2^{2n} - 1)$ es múltiplo de $2n = 2^{k+1}$, como queríamos.

Para finalizar, dejamos unos ejercicios para el lector.

Ejercicios

1. Hallar todos los números primos p tales que p^2+11 tiene exactamente 6 divisores positivos distintos.
2. Sean a, b, c enteros distintos de 0, con $a \neq c$, tales que $\frac{a}{c} = \frac{a^2+b^2}{c^2+b^2}$. Demostrar que $a^2 + b^2 + c^2$ no puede ser un número primo.
3. Demostrar que hay una infinidad de números que no son solitarios. (Ver Ejemplo 7 para la definición de número solitario.)
4. Sea n un entero positivo y sea $\pi(n)$ el producto de los divisores positivos de n. Demostrar que $\pi(n) = n^{\tau(n)/2}$.
5. Sea n un entero positivo. Demostrar que n es un cuadrado si y sólo si $\tau(n)$ es impar.
6. Sea n un entero positivo impar. Demostrar que $\sigma(n)$ es par si y sólo si n no es un cuadrado.
7. Determinar todos los enteros positivos n tales que $\tau(n) = \frac{n}{4}$.

Bibliografía

1. T. Andreescu, D. Andrica. *Number Theory. Structures, Examples and Problems.* Birkhäuser, 2009.
2. M. Baluna, R. Gologan. *Romanian Mathematical Competitions.* Romanian Mathematical Society, 2011.
3. M. Andronache, M. Baluna, R. Gologan, A. Eckstein, C. Popescu, D. Serbanescu. *Romanian Mathematical Competitions.* Romanian Mathematical Society, 2012.
4. Loren C. Larson. *Problem-Solving Through Problems.* Springer-Verlag, 1983.