Teorema de la división

Para $a \in Z$, $b \in N$. Existen unos únicos $q, r \in Z$ tales que $a = q \cdot b + r$, $0 \leq r < b$

A los números a, b, q y r se les llama *dividendo*, *divisor*, *cociente* y *resto*.

Demostración

1.- Demostramos que existen $q, r \in Z$ tales que $a = q \cdot b + r$, $0 \leq r < b$:

Sea bq el mayor múltiplo de b que es menor o igual que a, se cumple que $b \cdot q \leq a < b \cdot (q+1)$

Restando bq en la desigualdad anterior tenemos que

$$0 \leq a - bq < b(q+1) - bq = b \Rightarrow \text{ si tomamos } r = a - bq \text{ tendremos } 0 \leq r < b$$

2.- Demostremos la unicidad de q y r.

Si existiesen r_1, q_1, y r_2, q_2 con $a = bq_1 + r_1 = bq_2 + r_2$, entonces $b(q_2 - q_1) = r_1 - r_2$ y, por tanto, $b|(r_1 - r_2)$.

Pero, como $r_1, r_2 < b$, debe de ser $r_1 - r_2 = 0$

Viendo que $r_1 = r_2 \Rightarrow q_1 = q_2$.

Teorema de Bezout

Para a, b, enteros distintos de 0 y d = mcd(a,b), d es el entero positivo más pequeño que puede expresarse de la forma ax + by, con $x, y \in Z$.

Demostración:

Sea d el entero positivo más pequeño que puede expresarse de la forma $d = ax_1 + by_1$. Llegados a este punto tenemos que:

- d es divisor común de a y b:

Si d no dividiese al número a, se cumpliría $a = dq + r$ con $0 < r < d$ (algoritmo de la división). Por tanto $r = a - dq = a - (ax_1 + by_1) \cdot q = a \cdot (1 - x_1 \cdot q) + b(-y_1 \cdot q)$, con lo que vemos que r también se puede poner en la forma ax + by. Como $r < d$ y d era el menor positivo de esa forma tendremos que r = 0, por tanto d|a y, análogamente, podemos probar que d|b.

- d es el máximo común divisor:

Sea d' tal que d'|a, d'|b. Esto implica d´ |(ax + by), pero como d = ax + by entonces d´ |d.

Teorema fundamental de la aritmética

Sea $n>1, n \in Z$, entonces existen números primos $p_1, \ldots, p_k$ tales que $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ con $p_1 \leq p_2 \leq \ldots \leq p_k$

Esta factorización es única, es decir, si $n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$ con $q_1 \leq q_2 \leq \ldots \leq q_m$ entonces k = m y $q_i = p_i$ para i=1,2,..,k

Demostración :

Demostremos primero que todo número es factorizable.

Si el número es primo, la consecuencia es obvia. En otro caso, podrá ponerse de la forma n = ab con a, b < n. Repitiendo el procedimiento con a y b, obtenemos que n puede ponerse como producto de números cada vez menores. Como los números que aparecen son cada vez menores, este proceso ha de pararse alguna vez. En ese momento, n estará puesto como producto de números que no pueden factorizarse más, es decir, de números primos.

Veamos ahora que la factorización es única

Si $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ con $p_1 \leq p_2 \leq \ldots \leq p_k$ y $n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$ con $q_1 \leq q_2 \leq \ldots \leq q_m$, obtenemos $p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_m$, por lo que $p_1 | q_1 \cdot q_2 \cdot \ldots \cdot q_m$. Así pues, $p_1 | q_i$ para algún i. Esto quiere decir, teniendo en cuenta que q_i es primo, que $p_1 = q_i$. Podemos pues simplificar la expresión anterior y, razonando análogamente, demostrar que existe un j con que $p_2 = q_j$, y así sucesivamente. Reiterando el proceso, obtenemos que cada p_i es igual a un q_j distinto (y recíprocamente). Por tanto, k = m y los conjuntos $\{p_1, p_2, \ldots, p_k\}$ y $\{q_1, q_2, \ldots, q_m\}$ son iguales. Dado que ambos conjuntos están ordenados de forma creciente, tendremos que $q_i = p_i$ para cada i=1,2,..,k

Teorema El número de primos es infinito

Demostración:

Supongamos que $P = \{p_1, \ldots, p_t\}$, es el conjunto finito de números primos y hallemos la contradicción buscando un número que no sea divisible por ninguno de la lista

Sea $m = (p_1 \cdot p_2 \cdot \ldots p) + 1$. Como m no es divisible por ningún p_i, si estos fuesen los únicos que hay, no podría ponerse como producto de primos.

Teorema Sea $0 \neq a \in Z_n$. Entonces a es invertible $\Leftrightarrow$ mcd(a,n) = 1

Demostración:

a es invertible $\Leftrightarrow$ existe b con $a \cdot b = 1$ en $Z_n \Leftrightarrow$ existe b con $a \cdot b \equiv 1 \pmod{n} \Leftrightarrow$ existe b con $a \cdot b - 1 = kn \Leftrightarrow$ existen b, k con $a \cdot b - kn = 1$. Usando el Teorema de Bezout, esto se da si y sólo si m.c.d.(a,n) = 1

Teorema (de Euler)

Sean a y m dos números enteros con $m \geq 1$. Si mcd(a,m) = 1 se tiene que $a^{\phi(m)} \equiv 1 \pmod{m}$.

Demostración:

Sean $\{a_1, \ldots, a_{\phi(m)}\}$ los elementos invertibles de Z_m. Multiplicamos todos ellos por a y obtenemos un nuevo conjunto $\{aa_1, \ldots, aa_{\phi(m)}\}$.

Observemos que, como mcd(a,n) = 1, a es invertible en Z_m, por lo que los aa_i vuelven a ser invertibles. Por otro lado, deben de ser todos distintos ya que, si $aa_i = aa_j$, basta dividir por a para obtener $a_i = a_j$.

Por tanto, los $\{aa_1, \ldots, aa_{\phi(m)}\}$ son $\phi(n)$ elementos invertibles distintos de Z_m, por lo que deben de ser todos los elementos invertibles solamente que quizás en un orden distinto. Como el producto es conmutativo, se dará:

$$a_1 \ldots a_{\phi(m)} = aa_1 \ldots aa_{\phi(m)}$$

Basta simplificar ahora, dividiendo sucesivamente por a_1, por a_2,.. por $a_{\phi(m)}$ para obtener $a \ldots a = 1$. Por tanto $a^{\phi(m)} = 1$ en Z_m o, equivalentemente $a^{\phi(m)} \equiv 1 \pmod{m}$.