Conferencia 2 - Principios de la Teoría de Números

February 8, 2024

Lema. *Sea p primo, $a \in \mathbb{Z}$, si $p \nmid a$ entonces $(p, a) = 1$*

Lema. ***Lema de Euclides*** *Si p es un número primo y divide al producto de dos enteros positivos, entonces el número primo divide al menos a uno de los números.*

O sea, si $p|a * b$ entonces $p|a \vee p|b$.
O lo que es lo mismo, si $p|a * b$ y $(p, a) = 1$ entonces $p|b$.
Demostración
Supongamos, sin perdida de generalidad, que p es primo relativo con a (o sea $(a, b) = 1$) y que $p|ab$, entonces $ax + py = 1$ para x e y enteros.
Multiplicando b en ambos miembros se tiene $b(ax + py) = b$
luego $bax + bpy = b$
pero como $p|ab$ existe un r entero tal que $pr = ab$
entonces $prx + bpy = b$
luego $p(rx + by) = b$ y como $rx + by$ es entero entonces $p|b$

Teorema. *Sea p primo y $a_1, a_2, \ldots, a_n$ enteros, si $p|a_1 * a_2 * \ldots * a_n$ entonces existe $j \in \mathbb{Z}$ tal que $1 \leq j \leq n$ y $p|a_j$.*

Demostración
Para $n = 1$ es trivial
Asumamos $n = 2$ y que $p|a_1 * a_2$. Si se cumple $pa|a_1$ ya estaría demostrado. Ahora, si se supone que $p \nmid a_1$ entonces $p|a_2$ y también quedaría demostrado.
Ahora, supongamos que para $n = k$ se cumple, entonces para $n = k + 1$ como $p|a_1 * a_2 * \ldots * a_k * a_{k+1}$ si se tiene que $p|a_{k+1}$ ya quedaría demostrado. Pero, si $p \nmid a_{k+1}$ se sabe que sí se cumple que $p|a_1 * a_2 * \ldots * a_k$ (que fue lo que se supuso) y, por tanto, existe j, $1 \leq j \leq k + 1$ tal que $p|a_j$

Corolario. *Si $p, q_1, 1_2, \ldots, q_n$ son todos primos tales $p|q_1 * q_2 * \ldots * q_n$ entonces $p = q_k$ para algún k, $1 \leq k \leq n$*

Corolario. *Sean $a \in \mathbb{Z}$, $p \in \mathbb{Z}$, p primo y $k \in \mathbb{Z}_+$, si $p|a^k \Rightarrow (p|a \wedge p^k|a^k)$*

Demostración
Como $p|a^k$ entonces $p|a_1 * a_2 * \ldots * a_k$ donde cada $a_i = a$ con $1 \leq i \leq k$, luego, por el teorema anterior, existe un i tal que $p|a_i$ por lo que $p|a$ y, por tanto, $p^k|a^k$

Teorema. ***Teorema Fundamental de la Aritmética.*** *Todo número entero mayor que 1 se descompone en un producto de primos y si no se considera el orden de los factores entonces la descomposición es única.*

Demostración

Se debe demostrar, por una parte, que todo número se descompone en un producto de primos y, por otra parte, que dicha descomposición, sin importar el orden, es única.

Demostremos entonces que todo entero n, $n \geq 2$, se descompone en un producto de primos.

Para $n = 2$ se cumple pues 2 es primo.

Ahora, asumamos que para todos los enteros estrictamente menores que n se cumple que se descomponen en un producto de primos.

Entonces, si n es primo se cumple. Pero si n no es primo, entonces es un número compuesto y, por tanto, $n = a * b$ con $1 \leq a \leq b < n$ y, por lo supuesto, a y b se pueden expresar ambos como productos de primos, luego $n = a * b$ también lo es.

Demostremos ahora que la descomposición es única para todo entero n, $n \geq 2$.

Para $n = 2$ se cumple.

Ahora, asumamos que para todos los enteros estrictamente menores que n se cumple que su descomposición es única.

Sea $n = p_1 * p_2 * \ldots * p_R = q_1 * q_2 * \ldots * q_S$ donde p_i y q_j son primos con $1 \leq i \leq R$, $1 \leq j \leq S$, y están ordenados. Partiendo de esto se tiene que $p_1 | n \Rightarrow p_1 | q_1 * q_2 * \ldots * q_S$ luego $p_1 | q_j$ tal que $1 \leq j \leq S$. Entonces, como son primos $p_1 = q_j$ y cómo están ordenados $p_1 \geq q_1$.

De manera análoga se puede llegar a que $q_1 \geq p_1$ por lo que $p_1 = q_1$.

Entonces $\frac{n}{p_1} = p_2 * \ldots * p_R = q_2 * \ldots * q_S$ y como $\frac{n}{p_1} < n$ entonces, por lo supuesto, $\frac{n}{p_1}$ se descompone en factores de forma única, luego $R = S$ y $p_i = q_j$

Definición. *Se llama descomposición canónica de a a la siguiente* $a = p_1^{\alpha_1} * p_2^{\alpha_2} * \ldots * p_n^{\alpha_n}$ *donde, para* $1 \leq i \leq n$, $\alpha_i \geq 1$ *y es el orden de multiplicidad de* p_i, *y cada* p_i *es primo con* $p_1 < p_2 < \ldots < p_n$

Corolario. *Cualquier entero positivo n, $n > 1$ se puede escribir unívocamente en su forma canónica* $n = p_1^{\alpha_1} * p_2^{\alpha_2} * \ldots * p_n^{\alpha_n}$

Lema. *Todo número primo mayor que 3 se escribe de la forma* $6q \pm 1$ *para algún entero q*

Demostración

Como el número es entero entonces, por el **Algoritmo de la División**, se puede expresar como $6q + r$ con $0 \leq r < 6$

Ahora, como $6 = 2 * 3$ siendo 2 y 3 primos, si r toma los valores 0, 2 y 4 $6q + r$ sería par y, por tanto, no sería primo. Por su parte su parte si r es 3

$6q + r$ sería multiplo de 3. Entonces para que el número pueda ser primo r debería ser 1 o 5.

Para $r = 1$ se tiene $6q + 1$.

Para $r = 5$ se tendría entonces $6q + 5$ pero si se hace $q = k - 1$ entonces se tendría $6(k - 1) + 5{=}6k - 6 + 5 = 6k - 1$

Teorema. ***Teorema de Wilson****. Sea p entero mayor que 1, p es primo si y solo si $p|(p-1)! + 1$*

Teorema. ***Pequeño Teorema de Fermat****. Sea p primo y $a \in \mathbb{Z}$, entonces si $p \nmid a$ entonces $p|a^{p-1} - 1$*

Corolario. *Sea p primo y $a \in \mathbb{Z}$, entonces $p|a^p - a$*

Demostración

$p|a^p - a$ es $p|a(a^{p-1} - 1)$. Para p existen dos posibilidades: que divida o que no divida a a

Si $p|a$ entonces, evidentemente, p divide a $a(a^{p-1} - 1)$.

El otro caso es que $p \nmid a$ pero por el **Pequeño Teorema de Fermat** se cumple entonces que $p|a^{p-1} - 1$ y por tanto p divide a $a(a^{p-1} - 1)$.

Lema. *Dado cualquier entero positivo n, entonces existen n enteros consecutivos los cuales todos son números compuestos*

Demostración

Si se tiene la secuencia de n números:

$(n + 1)! + 2$, $(n + 1)! + 3$,. . . , $(n + 1)! + n$, $(n + 1)! + n + 1$

Entonces es evidente que:

$2|(n + 1)! + 2$, $3|(n + 1)! + 3$,. . . , $n|(n + 1)! + n$, $(n + 1)|(n + 1)! + n + 1$