DATE 23 . 03 . 20

Algebra Superior 2

Teo. El conjunto de números primos es infinito.

Antes de ver la demostración de este teorema recordemos lo siguiente:

Def. Sean A y B dos conjuntos. Se dice que A y B son equipotentes si existe $f: A \longrightarrow B$ biyectiva. En este caso escribimos $A \sim B$.

Def. Sea A un conjunto. Se dice que A es finito si existe $n \in \mathbb{N}$ talque $A \sim \{1,2,\dots,n\}$.

Def. Se dice que un conjunto es infinito si no es finito.

Un ejercicio muy bonito es ver que un conjunto es infinito si y solo si es equipotente con algún subconjunto propio.

Demostración de teorema: Supongamos que hay un número finito de números primos y sean éstos $p_1, p_2, \dots, p_n$.

Sea $q = p_1 p_2 \cdots p_n + 1$, entonces existe un número primo p que divide a q.

¿Por qué? Para contestar esta pregunta revisen el Teorema Fundamental de la Aritmética.

Ahora, p debe ser igual a p_i para alguna $1 \leq i \leq n$.

Entonces tenemos que $p_i \mid p_1 p_2 \cdots p_n + 1$ y como

$p_i \mid p_1 p_2 \cdots p_n$ entonces se sigue que $p_i \mid 1$ pero esto

es una contradicción. Por tanto podemos concluir que el conjunto de números primos no es finito ■

Nota: Si $p \in \mathbb{N}$ es un número primo y $p+2$ también lo es, entonces a la pareja $(p, p+2)$ se le conoce como una pareja de primos gemelos.

Ej: $(3,5)$, $(29,31)$

Es un problema abierto a la fecha en matemáticas si el conjunto de parejas de primos gemelos es infinito.

Teo. Sean $a, n \in \mathbb{N}$ ambos mayores que 1. Supongamos que $K = a^n - 1$ es un número primo, entonces $a = 2$ y n es primo.

Dem. Podemos escribir a $K = a^n - 1$ como

$$K = (a-1)(a^{n-1} + a^{n-2} + \cdots + 1)$$ y por tanto

$(a-1) \mid K$.

Si $a > 2$ entonces $a - 1 > 1$ y esto contradice el hecho de que K sea primo, por tanto $a = 2$.

Ahora, si n no es primo entonces $n = r \cdot s$ con $r, s \in \mathbb{N}$ ambos mayores que 1.

Así $K = 2^{r \cdot s} - 1 = (2^r)^s - 1$ y haciendo lo mismo que en el punto anterior podemos escribir a K como

$$K = (2^r)^s - 1 = (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + \cdots + 1).$$

Como $2^r > 2$ se sigue que K no es primo (¿Por qué?)

pero esto contradice nuestra hipótesis, por tanto n debe ser primo. ∎

Algunos ejercicios:

1. Utilice el teorema fundamental de la aritmética para encontrar el máximo común divisor de 360, 105 y 1078.

2. En clase se demostró que si $a, b, c \in \mathbb{N}$, entonces $(ca, cb) = c(a, b)$. Pruebe nuevamente el resultado apoyándose ahora sobre el teorema fundamental de la aritmética.