Tarea Tres.
Teoría de números uno.

Contreras Mendoza Ximena de la Luz

30 de marzo de 2020

Ejercicio 1.

1. Sea $a, b \in \mathbb{Z}$. Pruebe que $(a,b) = 1 \implies (a^n, b^n) = 1,\ \forall\ n \geqslant 0$

   Demostración. Sea $a = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ y $b = p_1^{\beta_1} \cdots p_s^{\beta_s}$ factorizaciones en primos respectivamente de a y b. Como $(a,b) = 1 \implies p_i^{\alpha_i} \neq p_j^{\beta_j}\ \forall\ 1 \leqslant i \leqslant t$ y $1 \leqslant j \leqslant s \implies a^k = p_1^{k\alpha_1} \cdots p_t^{k\alpha_t}$ y $b^k = p_1^{k\beta_1} \cdots p_s^{k\beta_s}$ tampoco tienen factores primos en común. □

2. Pruebe que $a \mid b \iff a^n \mid b^n,\ \forall\ n > 0$.

   Demostración. $\implies$) Por inducción sobre n.
   Base $n = 1$ $a \mid b \implies b = az$ p.a. $z \in \mathbb{Z}$.
   $b = b^1 = (az)^1 = az \quad \therefore a^1 \mid b^1$.

   H.I. Supongamos válido el resultado para $n = k$ P.d. válido para $n = k+1$.
   Por Hipótesis de inducción $b^k = (az)^k = a^k z^k$.
   Por otro lado $b^{k+1} = b^k b = b^k(az) = a^k z^k (ak) = a^k a z^k z = a^{k+1} z^{k+1}$ como $z^{k+1} \in \mathbb{Z}$ tenemos que $a^{k+1} \mid b^{k+1} \quad \therefore \quad$ si $a \mid b \implies a^n \mid b^n\ \forall\ n > 0$.

   $\impliedby$)$a^n \mid b^n\ \forall\ n > 0$ en particular para $n = 1, a^1 = a$ y $b^1 = b$ se cumple $a \mid b$. □

3. Sea $a \in \mathbb{Z}$ que no sea una n-ésima potencia de p, i.e. no existen $n > 0$ tal que $a = p^n$. Pruebe que $log_p(a)$ es irracional.

   Demostración. Observaciones: $log_p(a) = x \ \Leftrightarrow\ p^x = a$.
   1. $x \in \mathbb{R}$ y $x \notin \mathbb{Z}$.
   2. $a, p \in \mathbb{Z}$.
   3. $a \neq p^n\ \forall\ n > 0$
   Supongamos $x \in \mathbb{Q} \implies x = \frac{\alpha}{\beta}$ con $\alpha, \beta \in \mathbb{Z}, \beta \neq 0$, $log_p(a) = \frac{\alpha}{\beta} \Leftrightarrow p^{\frac{\alpha}{\beta}} = a \iff \sqrt[\beta]{p^\alpha} = a \iff$
   $p^\alpha = a^\beta \rightarrow\leftarrow$ pues $a \neq p^n\ \forall\ n > 0$
   La contradicción viene de suponer que $x \in \mathbb{Q}$. Por lo tanto x es irracional. □

Ejercicio 2.

1. Para $r \in \mathbb{Q}$ arbitrario define la parte entera de r como $[r] := máx\{k \in \mathbb{Z} : k \leq r\}$. Con esta definición pruebe que
   $\nu_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$
   Tienen que probar que la serie es convergente para que tenga sentido la igualdad.

   Demostración. Primero probaré que $\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$ converge.
   Afirmación: $\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$ en realidad es una suma finita, $\exists k \in \mathbb{N}$ tal que $\ \forall\ n \geqslant k, \left[\frac{n}{p^k}\right] = 0$

   Prueba: Sea $a_n = \left[\frac{m}{p^n}\right]$. Mi sucesión de a_n es estrictamente decreciente i.e. $a_n > a_{n+1}\ \forall\ n \geqslant 1$.
   $p > 1 \implies p^{n+1} > p^n\ \forall\ n \implies \frac{1}{p^{n+1}} < \frac{1}{p^n} \implies \frac{m}{p^{n+1}} < \frac{m}{p^n} \implies \left[\frac{m}{p^{n+1}}\right] \leqslant \left[\frac{m}{p^n}\right]$

   Hay dos casos, que $\frac{m}{p^{n+1}}, \frac{m}{p^n} \in \mathbb{Q}$ pero que $\frac{m}{p^{n+1}}, \frac{m}{p^n} \notin \mathbb{Z}$.
   1. $\exists a \in \mathbb{Z}$ tal que $a - 1 < \frac{m}{p^{n+1}} < a < \frac{m}{p^n} \implies a - 1 = \left[\frac{m}{p^{n+1}}\right] < a = \left[\frac{m}{p^n}\right]$.

2. No existe un entero entre $\frac{m}{p^{n+1}}$ y $\frac{m}{p^n}$ entonces $\left[\frac{m}{p^{n+1}}\right] = \left[\frac{m}{p^n}\right]$ por lo tanto $\left[\frac{m}{p^{n+1}}\right] \leqslant \left[\frac{m}{p^n}\right]$.
Si ambos $\left[\frac{m}{p^{n+1}}\right], \left[\frac{m}{p^n}\right] \in \mathbb{Z} \Longrightarrow \left[\frac{m}{p^{n+1}}\right] \leqslant \left[\frac{m}{p^n}\right]$.

Si alguno de ellos es entero y el otro iracional:
1. $\left[\frac{m}{p^{n+1}}\right] \in \mathbb{Z}$ y $\left[\frac{m}{p^n}\right] \notin \mathbb{Z}$ entonces $\frac{m}{p^{n+1}} = \left[\frac{m}{p^{n+1}}\right]; \frac{m}{p^{n+1}} < \frac{m}{p^n}$.
Por otro lado $\frac{m}{p^{n+1}} = \left[\frac{m}{p^n}\right] \therefore \left[\frac{m}{p^{n+1}}\right] \leqslant \left[\frac{m}{p^n}\right]$.
2. $\left[\frac{m}{p^n}\right] \in \mathbb{Z}$ y $\left[\frac{m}{p^{n+1}}\right] \notin \mathbb{Z}$ entonces $\frac{m}{p^n} = \left[\frac{m}{p^n}\right]; \left[\frac{m}{p^{n+1}}\right] < \frac{m}{p^{n+1}} < \frac{m}{p^n} = \left[\frac{m}{p^n}\right] \therefore \left[\frac{m}{p^{n+1}}\right] \leqslant \left[\frac{m}{p^n}\right]$.

Por lo tanto para toda n, $\left[\frac{m}{p^n}\right]$ son enteros positivos decrecientes, por el P.B.O. debe de haber un mínimo. El cero es dicho mínimo.
Si $p > m \Longrightarrow \frac{m}{p} < 1 \Longrightarrow \left[\frac{m}{p}\right] = 0$.
Si $p < m \Longrightarrow \frac{m}{p} > 1$, como $\frac{m}{p} > \frac{m}{p^2} > \ldots > \frac{m}{p^n}$.
Sea $\varepsilon = 1$
como $\lim_{n\to\infty}(\frac{m}{p^n}) = 0 \Longrightarrow \exists N \in \mathbb{N}$ talque si $n \geqslant N \Longrightarrow |\ \frac{m}{p^n}\ | < \varepsilon = 1$. A partir de N se cumple que $1 > \frac{m}{p^n}$ si $n \geqslant N$
$\therefore \left[\frac{m}{p^n}\right] = 0$.
Por lo tanto $\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$ es una suma finita, pues a partir de cierta k, sumo puros ceros, por lo tanto $\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$ converge.

Ahora probaré la igualdad: $\nu_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$.

Lema : $q = \left[\frac{n}{m}\right]$. Donde q es el número de múltiplos de m menores que n.
Prueba: Por el Algoritmo de la división, $n = qm + r$ --→ (1) con $0 \leqslant r < q$ entonces el mayor múltiplo de m hasta n es qm. Todos los múltiplos de m hasta n son $m, 2m, 3m, ..., qm$. Dividiendo (1) por m tenemos $\frac{n}{m} = q + \frac{r}{m} \Longrightarrow \left[\frac{n}{m}\right] = \left[q + \frac{r}{m}\right]$ pero $0 \leqslant \frac{r}{m} < 1 \therefore \left[q + \frac{r}{m}\right] = q$. Como qm es el mayor multiplo de m hasta n, entonces $q = \left[\frac{n}{m}\right]$ $\star$

$\left[\frac{n}{m}\right]$ es el mayor multiplo de n hasta p^k entonces es el número de enteros $0 < m \leqslant n$ multiplos de p^k. Veamos que cualquier entero m tal que $0 < m \leqslant n$ que es divisible por p^j y no por p^{j+1} debe ser contado exactamente j veces i.e. una vez en $\left[\frac{n}{p}\right]$, una vez en $\left[\frac{n}{p^2}\right]$, ... ,una vez en $\left[\frac{n}{p^j}\right]$. Son todos los múltiplos de p como factor de $n!$ por lo tanto $\nu_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$. □

Ejercicio 3.

Pruebe que no hay polinomios con coeficientes enteros que generen números primos. Más precisamente pruebe que $\forall\ f \in \mathbb{Z}[x]$ $\exists n \in \mathbb{Z}$ tal que $f(n)$ es compuesto.

Demostración. Supongamos que $\exists\ f \in \mathbb{Z}[x]$ tal que $\forall\ n \in \mathbb{Z}, f(n)$ es primo.
Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, un polinomio de grado n, con coeficientes enteros, tal que, da valores primos para cualquier número entero.
En particular $f(1) = a_n + a_{n-1} + ... + a_1 + a_0 = p$, primo. Calculemos $f(1 + kp)$ con $k \in \mathbb{Z}$.
$f(1 + kp) = a_n(1 + kp)^n + a_{n-1}(1 + kp)^{n-1} + ... + a_1(1 + kp) + a_0$.
Utilizando el binomio de Newton, $\sum_{i=1}^{n} = \frac{n!}{i!(n-i)!}(1)^{n-k}(kp)^i = \sum_{i=1}^{n} = \frac{n!}{i!(n-i)!}(kp)^i$
Observemos que todos los términos son múltiplos de p, excepto posiblemente $a_n, a_{n-1}, ..., a_1, a_0$ pero
$a_n + a_{n-1} + ... + a_1 + a_0 = p$ así $f(1 + kp)$ es un múltiplo de p. Digamos mp para alguna $m \in \mathbb{Z}$.
Como $f(x)$ da valores primos para toda $n \in \mathbb{Z} \Longrightarrow f(1 + kp) = mp$ es primo, eso implica que $m = 1$. Por lo tanto $f(1 + kp) = p$ con $k \in \mathbb{Z}$ arbitraria, es decir f toma el valor p para una cantidad infinita de valores.
Sea $g(x) = f(x) - p$, las raíces de $g(x)$ serian $1 + kp$, para cualquier $k \in \mathbb{Z}$ i.e. $g(x)$ tendría una cantidad infinita de raíces. →←
Es una contradicción al Teorema Fundamental del Álgebra. La contradicción surge de suponer que existe un polinomio en $\mathbb{Z}[x]$ tal que $\forall n \in \mathbb{Z}, f(n)$ es primo. Por lo tanto debe pasar que $\forall\ f \in \mathbb{Z}[x]$ $\exists n \in \mathbb{Z}$ tal que $f(n)$ es compuesto.

□

[n/p^n] <= $n/p^n, nu_p(n!)$