# Tarea Dos
# Teoría de números uno.

Contreras Mendoza Ximena de la Luz

25 de marzo de 2020

## Ejercicio 1.

Pruebe que para todo natural $n > 1$, el conjunto $\{n+1, n+2, \ldots, n!+1\}$ contiene un primo, i.e. $\mathcal{P} \cap [n+1, n!+1] \neq \emptyset$ para toda $n > 1$. Use este hecho para dar otra prueba de la infinitud de los primos.

*Demostración.* P.d. $\mathcal{P} \cap [n+1, n!+1] \neq \emptyset$.
Recordemos la definición de $\pi(x) : \mathbb{R} \longrightarrow \mathbb{N}$
$\pi(x) = \#\mathcal{P} \cap [0, x]$. Observaciones:
1) $0 < n+1 \leq n!+1 \ \forall \ n > 1$
2) Para toda $n > 1$, el intervalo $[n+1, n!+1] \subset [0, n!+1] \Longrightarrow \mathcal{P} \cap [n+1, n!+1] \subset \mathcal{P} \cap [0, n!+1]$
3) Para toda $n > 1$, el intervalo $[0, n+1] \subset [0, n!+1] \Longrightarrow \mathcal{P} \cap [0, n+1] \subset \mathcal{P} \cap [0, n!+1]$

Afirmación: $\mathcal{P} \cap [n+1, n!+1] = (\mathcal{P} \cap [0, n!+1] - \mathcal{P} \cap [0, n+1]) \cup \mathcal{P} \cap \{n+1\}$.

Prueba: $\subseteq$) Sea $x \in \mathcal{P} \cap [n+1, n!+1] \Longrightarrow x \in \mathcal{P}$ y $x \in [n+1, n!+1] \subset [0, n!+1] \Longrightarrow x \in \mathcal{P}$ y $x \in [0, n!+1]$ entonces $x \in (\mathcal{P} \cap [0, n!+1] - \mathcal{P} \cap [0, n+1]) \cup \mathcal{P} \cap \{n+1\}$.

$\supseteq$) Sea $x \in (\mathcal{P} \cap [0, n!+1] - \mathcal{P} \cap [0, n+1]) \cup \mathcal{P} \cap \{n+1\} \Longrightarrow x \in (\mathcal{P} \cap [0, n!+1] - \mathcal{P} \cap [0, n+1])$ ó $x \in \mathcal{P} \cap \{n+1\}$. Si $x \in \mathcal{P} \cap \{n+1\} \Longrightarrow n+1$ es primo $\Longrightarrow x \in \mathcal{P} \cap [n+1, n!+1]$.
Si $x \in (\mathcal{P} \cap [0, n!+1] - \mathcal{P} \cap [0, n+1]) \Longrightarrow x \in \mathcal{P} \cap [0, n!+1]$ y $x \notin \mathcal{P} \cap [0, n+1]) \Longrightarrow x \in \mathcal{P}$ y $x \in [0, n!+1]$ y $x \notin [0, n+1] \Longrightarrow x \in (n+1, n!+1]$. Aquí aparece un problema pues me quedó $\mathcal{P} \cap (n+1, n!+1]$ y yo quiero $\mathcal{P} \cap [n+1, n!+1]$. En realidad no es un problema. Pues solo abría que fijarse si $n+1$ es primo o no.
1. Si es primo, $n+1$ está en $\mathcal{P} \cap [0, n!+1] - \mathcal{P} \cap [0, n+1]$ y está en $\mathcal{P} \cap \{n+1\}$ entonces lo quito y lo agrego, por lo tanto $\mathcal{P} \cap (n+1, n!+1]$ en realidad si queda $\mathcal{P} \cap [n+1, n!+1]$.
2. Si $n+1$ no es primo entonces no está en $\mathcal{P} \cap [0, n!+1] - \mathcal{P} \cap [0, n+1]$ y no está en $\mathcal{P} \cap \{n+1\}$ entonces no le estoy quitando nada *i.e.* $\mathcal{P} \cap [0, n+1) = \mathcal{P} \cap [0, n+1] \Longrightarrow \mathcal{P} \cap (n+1, n!+1] = \mathcal{P} \cap [n+1, n!+1]$.
$\therefore$ si $x \in (\mathcal{P} \cap [0, n!+1] - \mathcal{P} \cap [0, n+1]) \cup \mathcal{P} \cap \{n+1\} \Longrightarrow x \in \mathcal{P} \cap [n+1, n!+1]$.

Por otro lado $\pi(x)$ es no decreciente, entonces si $n+1 \leq n!+1, \ \forall \ n > 1 \Longrightarrow \pi(n+1) \leq \pi(n!+1) \Longrightarrow 0 \leq \pi(n!+1) - \pi(n+1)$ P.d. $\pi(n!+1) - \pi(n+1) > 0$.
Es decir para que $\mathcal{P} \cap [n+1, n!+1] = (\mathcal{P} \cap [0, n!+1] - \mathcal{P} \cap [0, n+1]) \cup \mathcal{P} \cap \{n+1\} \neq \emptyset$ basta ver que $\exists p_i \in \mathcal{P} \cap [0, n!+1]$ tal que $p_i \notin \mathcal{P} \cap [0, n+1]$. Tenemos que:
$\#\mathcal{P} \cap [n+1, n!+1] = \pi(n!+1) - \pi(n+1) + 1$, si $n+1 \in \mathcal{P}$ ó
$\#\mathcal{P} \cap [n+1, n!+1] = \pi(n!+1) - \pi(n+1)$, si $n+1 \notin \mathcal{P}$.
Estoy tomando valores de $\pi(x)$ (enteros positivos) saltados en uno *i.e.* $\pi(n+1), \pi(n+2), ..., \pi(n!+1)$ y por la observación 1) $0 < n+1 \leq n!+1 \ \forall \ n > 1$, se da la igualdad solamente cuando $n = 2$, por lo tanto si $n > 2$ la desigualdad es estricta *i.e.* $n+1 < n!+1 \Longrightarrow \pi(n+1) < \pi(n!+1) \therefore \pi(n!+1) - \pi(n+1) > 0$. Así $\#\mathcal{P} \cap [n+1, n!+1] > 0$. Por lo tanto $\mathcal{P} \cap [n+1, n!+1] \neq \emptyset$
Faltaría ver que pasa cuando $n = 2$ en este caso nuestro intervalo $[n+1, n!+1]$ es simplemente un punto el 3, por lo tanto $\mathcal{P} \cap 3 = 3 \neq \emptyset$.

Para dar otra prueba de la infinitud de los primos. Como $\mathcal{P} \cap [n+1, n!+1] \neq \emptyset$ para todo natural $n > 1$, tenemos que el intervalo $[n+1, n!+1]$ tiende a infinito cuando n tiende a infinito, pero como $n+1 < n!+1 \ \forall \ n > 2$ siempre tendremos un intervalo que también crece en longitud. Por lo tanto siempre que "nos acercamos" a infinito encontramos primos, pues $\mathcal{P} \cap [n+1, n!+1] \neq \emptyset$. $\square$

## Ejercicio 2.

Pruebe que existen intervalos arbitrariamente grandes donde no aparece un número primo, *i.e.* pruebe que para toda $n > 0$ existen reales $x, y$ tales que $\mid x - y \mid > n$ y que $\mathcal{P} \cap [x, y] = \emptyset$

*Demostración.* Supongamos que no. Es decir que $\exists n_0 \in \mathbb{N}$ tal que para todo $x, y \in \mathbb{R}$ tales que $\mid x - y \mid > n_0$, $\mathcal{P} \cap [x, y] \neq \emptyset$. Entonces dos primos consecutivos no pueden distar más que $n_0$. Entre 1 y $N$ hay por lo menos $\frac{N}{n_0}$ primos, entonces $\pi(x)$ siempre es al menos $\frac{x}{n_0}$. Entonces tenemos esta desigualdad $\frac{\pi(x)}{x} \geq \frac{1}{n_0} \ \forall \ x \dashrightarrow (1)$.
Por otro lado sabemos que $\frac{\pi(x)}{x} \approx \frac{1}{ln(x)} \implies \frac{\pi(x)}{x} \leqslant \frac{2}{ln(x)} \ \forall \ x \dashrightarrow (2)$
Juntando (1) y (2) tenemos $\frac{1}{n_0} \leqslant \frac{\pi(x)}{x} \leqslant \frac{2}{ln(x)} \ \forall \ x \implies n_0 \geq \frac{ln(x)}{2} \ \forall \ x \quad \rightarrow\leftarrow$
Pues $\frac{ln(x)}{2}$ tiende a infinito cuando $x$ tiende a infinito. La contradicción surge de suponer intervalos más grandes que un tamaño fijo. Por lo tanto para todo $n > 0$ existen intervalos de tamaño mayor que $n$ que no contienen primos. □

## Ejercicio 3.

1. Sea $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ la factorización de $a$ en primos. Pruebe que $a$ es una n-ésima potencia de otro entero si y solo si $n \mid \alpha_i \ \forall \ i \in \{1, ..., s\}$.

   *Demostración.* $\Rightarrow$) $a = b^n$ para algún $b \in \mathbb{Z}$. P.d. $n \mid \alpha_i \ \forall \ i \in \{1, ..., s\}$
   $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Como $b \in \mathbb{Z}$ entonces $b$ tiene una factorización en primos, sea $b = p_1^{\beta_1} \cdots p_t^{\beta_t}$ dicha factorización. Luego tenemos que
   $b = p_1^{\beta_1} \cdots p_t^{\beta_t} \implies b^n = (p_1^{\beta_1} \cdots p_t^{\beta_t})^n = p_1^{n\beta_1} \cdots p_t^{n\beta_t}$
   Por otro lado $a = b^n$ entonces $p_1^{\alpha_1} \cdots p_s^{\alpha_s} = p_1^{n\beta_1} \cdots p_t^{n\beta_t}$ como $\mathbb{Z}$ es DFU entonces debe pasar que $s = t$ y para toda $i$, $\alpha_i = n\beta_i$ por lo tanto $n \mid \alpha_i \ \forall \ i$

   $\Leftarrow$) $n \mid \alpha_i \ \forall \ i \in \{1, ..., s\}$ P.d. $a = b^n$ para algún $b \in \mathbb{Z}$.
   $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \implies$ (como $n \mid \alpha_i \ \forall \ i$) $\sqrt[n]{a} = p_1^{\frac{\alpha_1}{n}} \cdots p_s^{\frac{\alpha_s}{n}}$. Sea $b = p_1^{\beta_1} \cdots p_s^{\beta_s}$, donde
   $\beta_1 = \frac{\alpha_1}{n}, \beta_2 = \frac{\alpha_2}{n}, \ ..., \beta_s = \frac{\alpha_s}{n}$ entonces $\sqrt[n]{a} = b$, entonces
   $b^n = (p_1^{\beta_1} \cdots p_s^{\beta_s})^n = p_1^{n\beta_1} \cdots p_s^{n\beta_s} =_{\triangleleft} p_1^{\alpha_1} \cdots p_s^{\alpha_s} = a.$ ($_{\triangleleft}$ por definición de $\beta_i$)
   $\therefore a = b^n$ con $b \in \mathbb{Z}$ □

2. Pruebe que $\sqrt[n]{a} \in \mathbb{Q}$ si y solo si $a$ es una n-ésima potencia, es decir que $a = b^n$ para alguna $b \in \mathbb{Z}$.

   *Demostración.* $\Rightarrow$) Si $a = b^n$ p.a. $b \in \mathbb{Z} \implies \sqrt[n]{a} = b$ por lo tanto $\sqrt[n]{a} \in \mathbb{Z}$
   $\therefore \sqrt[n]{a} \in \mathbb{Q}$

   $\Leftarrow$) Si $\sqrt[n]{a} \in \mathbb{Q}$ entonces $\sqrt[n]{a} = \frac{p}{q}$ donde $p, q \in \mathbb{Z}$ y $q \neq 0$.
   Entonces $a = \left(\frac{p}{q}\right)^n$, como $a \in \mathbb{Z}$ esto forza a que $\frac{p}{q} \in \mathbb{Z} \implies q \mid p \implies p = qk$ p.a. $k \in \mathbb{Z}$ entonces $\left(\frac{p}{q}\right)^n = \left(\frac{qk}{q}\right)^n = \frac{q^n k^n}{q^n} = k^n$ por lo tanto $a = \left(\frac{p}{q}\right)^n = k^n$ con $k \in \mathbb{Z}$.
   $\therefore a$ es una n-ésima potencia. □

   Otra prueba, usando el ejercicio 4.

   Prueba. Supongamos $\sqrt[n]{a}$, raíz de $f(x)$ polinomio mónico en $\mathbb{Z}[x]$. Por el ejercicio 4. tenemos que $\sqrt[n]{a} \in \mathbb{Z}$ ó $\sqrt[n]{a} \in \mathbb{R} \setminus \mathbb{Q}$.
   Si $\sqrt[n]{a} \in \mathbb{R} \setminus \mathbb{Q}$. No hay nada que hacer.
   Si $\sqrt[n]{a} \in \mathbb{Z} \subset \mathbb{Q} \implies \sqrt[n]{a} = k \implies a = k^n$ por lo tanto $a$ es una n-ésima potencia.

## Ejercicio 4.

Sea $f(x) = x^n + \cdots + a_1x + a_0$ un polinomio mónico con coeficientes en enteros. Supongamos que $\alpha \in \mathbb{R}$ es una raíz de $f(x)$. Pruebe que $\alpha \in \mathbb{Z}$ ó $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Si quitamos la hipótesis de que $f(x)$ sea mónico, el ejercicio deja de ser cierto. Da un ejemplo de un polinomio $f(x)$ no mónico, con una raíz $\alpha$ que no es ni entero ni irracional.

*Demostración.* Sea $\alpha \in \mathbb{R}$ raíz de $f(x) = x^n + ... + a_1x + a_0$, polinomio mónico con coeficientes enteros.
Si $\alpha$ es irracional, no hay nada que hacer.
Supongamos $\alpha$ racional. Entonces podemos ver a $\alpha = \frac{p}{q}$, con $p, q \in \mathbb{Z}, q \neq 0$ y podemos pedir que $(p, q) = 1$.
Como $\alpha$ es raíz de $f(x) \Longrightarrow \alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0 \Longrightarrow \alpha^n = -(a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0)$ $\dashrightarrow$ (1).
Multiplicamos a (1) por $q^n$, entonces $q^n\alpha^n = -q^n(a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0) \Longrightarrow$
$q^n\alpha^n = q^n\left(\frac{p}{q}\right)^n = p^n = -q^n(a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0) = -(a_{n-1}q^n\left(\frac{p}{q}\right)^{n-1} + ... + a_1q^n\left(\frac{p}{q}\right) + a_0q^n)$
$= -(a_{n-1}qp^{n-1} + ... + a_1q^{n-1}p + a_0q^n)$ Por lo tanto $p^n = -(a_{n-1}qp^{n-1} + ... + a_1q^{n-1}p + a_0q^n)$.

Si $q > 1$ el lado derecho es un multiplo de $q$ pero $p^n$ no es multiplo de $q$ pues $(p, q) = 1$. Por lo tanto esto obliga a que $q = 1$. Por lo tanto $\alpha$ es entero. □

Ejemplo: $g(x) = 3x + 1$, $\alpha = -\frac{1}{3}$ es raíz de $g(x)$. $\alpha \notin \mathbb{Z}$ y $\alpha \notin \mathbb{R} \setminus \mathbb{Q}$