



Pontificia Universidad Católica de Chile  
Facultad de Matemáticas  
2° semestre 2020

## Ayudantía 02

21 de Agosto

MAT2225 - Teoría de Números

- 1) Sean  $a, b$  enteros positivos. Asuma que  $\text{mcd}(a, b) + \text{mcm}(a, b) = a + b$ .  
Pruebe que  $a \mid b$  o  $b \mid a$ .  
*Puede usar (por la lista de problemas) que  $\text{mcm}(a, b) \cdot \text{mcd}(a, b) = ab$ .*

*Demostración.* Sea  $k = \text{mcd}(a, b)$ . Luego,  $a = a'k$ ,  $b = b'k$  y  $\text{mcm}(a, b) = a'b'k$ . Reescribiendo la igualdad, se tiene

$$k + ka'b' = ka' + kb'.$$

Como  $k \neq 0$ , lo anterior es equivalente a

$$1 + a'b' = a' + b'.$$

Moviendo todo a la izquierda se tiene

$$a'b' - a' - b' + 1 = 0.$$

Factorizando, se llega a

$$(a' - 1)(b' - 1) = 0$$

Esto implica que  $a' = 1$  o  $b' = 1$ . Si  $a' = 1$ , entonces  $a = \text{mcd}(a, b)$  y  $a \mid b$ . Si  $b' = 1$  es análogo, por lo que se tiene lo pedido. ■

- 2) Pruebe que hay infinitos primos de la forma  $4k + 3$ .

Supongamos que hay una cantidad finita de primos de la forma  $4k + 3$ :  $p_1 = 3, p_2 = 7, \dots, p_j$ . Consideremos  $N = 4p_2p_3 \dots p_j + 3$ . Notar que  $3 \nmid N$ , ya que si pasara, se tendría que  $3 \mid 4p_2p_3 \dots p_j$ ,  $\rightarrow \leftarrow$  (recordar que  $p_1 = 3$ , por lo que no aparece en el producto). Similarmente, ningún primo  $p_i$  (con  $2 \leq i \leq j$ ) divide a  $N$ , ya que si pasara entonces se tendría que  $p_i \mid 3$ .

Por teorema fundamental de la aritmética, sabemos que  $N = q_1^{\alpha_1} \cdots q_n^{\alpha_n}$ , donde  $q_i$  es primo para todo  $i$ . Basta mostrar que algún  $q_i$  es de la forma  $4k + 3$ , ya que no puede ser ningún  $p_i$  ( $1 \leq i \leq j$ ). Para esto, basta ver que si todos los primos fueran de la forma  $4k + 1$  el producto también lo es,  $\rightarrow \leftarrow$ .

Por lo tanto, existen infinitos primos de la forma  $4k + 3$ .

- 3) a) (*Fórmula de Legendre/de De Polignac*) Sea  $p$  un primo y  $n$  natural. Muestre que

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor,$$

donde  $\lfloor x \rfloor$  denota la función piso de  $x$ .

*Demostración.* Notar que solo los múltiplos de  $p$  añaden un factor de  $p$  a  $n!$ :  $p, 2p, 3p, \dots, \left\lfloor \frac{n}{p} \right\rfloor p$ . Así, hay  $\left\lfloor \frac{n}{p} \right\rfloor$  múltiplos de  $p$ . De estos, hay que contar de nuevo los que aportan al menos 2 veces  $p$  al producto, los múltiplos de  $p^2$ , de los que hay  $\left\lfloor \frac{n}{p^2} \right\rfloor$ , y así sucesivamente. Como eventualmente  $p^k > n$  la suma es finita, por lo que se necesitan solo una cantidad finita de pasos y se tiene lo pedido. ■

- b) Determine con cuantos ceros termina  $2020!$ .

*Solución.* Notar que lo pedido es equivalente a ver la mayor potencia de 10 que divide a  $2020!$ . Como  $10 = 2 \cdot 5$ , basta ver cuantos  $2s$  y  $5s$  hay en la factorización prima. Por la parte anterior, tenemos que

$$\begin{aligned} \nu_2(2020!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{2020}{2^k} \right\rfloor \\ &= \left\lfloor \frac{2020}{2} \right\rfloor + \left\lfloor \frac{2020}{4} \right\rfloor + \left\lfloor \frac{2020}{8} \right\rfloor + \left\lfloor \frac{2020}{16} \right\rfloor + \left\lfloor \frac{2020}{32} \right\rfloor + \left\lfloor \frac{2020}{64} \right\rfloor \\ &\quad + \left\lfloor \frac{2020}{128} \right\rfloor + \left\lfloor \frac{2020}{256} \right\rfloor + \left\lfloor \frac{2020}{512} \right\rfloor + \left\lfloor \frac{2020}{1024} \right\rfloor + \left\lfloor \frac{2020}{2048} \right\rfloor + \underbrace{\left\lfloor \frac{2020}{4096} \right\rfloor}_{=0} \\ &= 1010 + 505 + 252 + 126 + 63 + 31 + 15 + 7 + 3 + 1 \\ &= 2013. \end{aligned}$$

Del mismo modo,

$$\begin{aligned}
\nu_5(2020!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \\
&= \left\lfloor \frac{2020}{5} \right\rfloor + \left\lfloor \frac{2020}{25} \right\rfloor + \left\lfloor \frac{2020}{125} \right\rfloor + \left\lfloor \frac{2020}{625} \right\rfloor + \left\lfloor \frac{2020}{3125} \right\rfloor + \underbrace{\dots}_{=0} \\
&= 404 + 80 + 16 + 3 \\
&= 503.
\end{aligned}$$

Por lo tanto,  $2020!$  termina con  $\min(\nu_2(2020!), \nu_5(2020!)) = 503$  ceros. ■

- 4) a) Muestre que  $\nu_p(\text{mcd}(a, b)) = \min(\nu_p(a), \nu_p(b))$ .

*Demostración.* Sin pérdida de generalidad, supongamos que  $\nu_p(a) \leq \nu_p(b)$ . Notar que para cualesquiera  $x, y$  enteros, se tiene que

$$ax + by = p^{\nu_p(a)} a'x + p_p^{\nu}(a)b'y = p_p^{\nu}(a) \underbrace{(a'x + b'y)}_{\in \mathbb{Z}}.$$

Luego,  $p^{\nu_p(a)} \mid \text{mcd}(a, b)$  y  $\nu_p(\text{mcd}(a, b)) \geq \nu_p(a) = \min(\nu_p(a), \nu_p(b))$  por definición.

Para probar que  $\nu_p(\text{mcd}(a, b)) \leq \nu_p(a)$ , basta ver que  $p^{\nu_p(\text{mcd}(a, b))} \mid \text{mcd}(a, b) \mid a$ , por lo que  $p^{\nu_p(\text{mcd}(a, b))} \mid a$  y la desigualdad se tiene a partir de la definición.

Como  $\nu_p(\text{mcd}(a, b)) \geq \min(\nu_p(a), \nu_p(b))$  y  $\nu_p(\text{mcd}(a, b)) \leq \min(\nu_p(a), \nu_p(b))$ , se tiene la igualdad buscada. ■

- b) Pruebe que  $\nu_p(a \pm b) \geq \min(\nu_p(a), \nu_p(b))$  para todos  $a, b \in \mathbb{P}$ , y muestre que se transforma en igualdad si las valuaciones de  $a$  y  $b$  son distintas.

*Demostración.* Sin perder generalidad, supongamos que  $\nu_p(a) \leq \nu_p(b)$ . Luego,  $a = p^{\nu_p(a)} \cdot a'$  y  $b = p^{\nu_p(a)} \cdot b'$ , donde  $p \nmid a'$ . Re-escribiendo  $a \pm b$ , se tiene

$$a \pm b = p^{\nu_p(a)} \underbrace{(a' \pm b')}_{\in \mathbb{Z}}.$$

Esto muestra la desigualdad. Ahora, si tienen valuaciones distintas, entonces además podemos decir que  $b = p^{\nu_p(a)} \cdot pb'$  (ya que  $\nu_p(a) \leq \nu_p(b)$ ). Luego, al re-escribir se tiene

$$a \pm b = p^{\nu_p(a)}(a' \pm pb').$$

Si mostramos que  $p^{\nu_p(a)+1} \nmid p^{\nu_p(a)}(a' \pm pb')$  estamos listos. Supongamos que ocurre lo contrario. Es decir, existe un entero  $x$  tal que

$$p^{\nu_p(a)+1}x = p^{\nu_p(a)}(a' \pm pb').$$

Dividiendo por  $p^{\nu_p(a)}$  a ambos lados, se llega a

$$px = a' \pm pb',$$

lo que se puede re-escribir como  $p(x \mp b') = a'$ . Pero  $p \nmid a'$ ,  $\rightarrow \leftarrow$ . Así, se tiene la igualdad buscada. ■

**Bonus:** (Putnam 2000 - B2) Sean  $n \geq k$  enteros positivos. Muestre que  $\binom{n}{k} \cdot \frac{(n,k)}{n}$  es natural.

*Hint:* Se puede hacer solo con materia de la semana pasada, o usando valuaciones.

*Demostración 1.* La expresión anterior no es natural si y solo si existe un primo  $p \mid n$  que se mantiene en el denominador al realizar la multiplicación. Luego, consideremos dos casos:

- $\nu_p(n) = \nu_p(k)$ : Luego,  $\nu_p((n,k)) = \nu_p(n)$  y el primo desaparece del denominador (ya que se cancela con  $(n,k)$ ).
- $\nu_p(n) \neq \nu_p(k)$ : Notar que  $\binom{n}{k} = \frac{n}{n-k} \binom{n-1}{k-1}$ . Luego,

$$\binom{n}{k} \cdot \frac{(n,k)}{n} = \binom{n-1}{k-1} \cdot \frac{(n,k)}{n-k}$$

Como  $\nu_p((n,k)) = \nu_p(n-k)$  por la pregunta anterior y  $\nu_p\left(\binom{n-1}{k-1}\right) \geq 0$ , también se tiene que  $p$  desaparece del denominador.

Uniando ambos casos se tiene lo pedido. ■

*Demostración 2.* Notar que  $(n, k) = an + bk$ , con  $a, b \in \mathbb{Z}$ . Trabajando un poco la expresión, se tiene

$$\binom{n}{k} \cdot \frac{(n, k)}{n} = \binom{n}{k} \cdot \frac{an + bk}{n} = a \binom{n}{k} + b \binom{n-1}{k-1}.$$

Esto muestra que es entero. Como es claramente no-negativo (ya que  $(n, k)$ ,  $n$  y  $\binom{n}{k}$  son no-negativos), se tiene lo pedido. ■