Factoriales!

Ezra Guerrero Alvarez

4 de enero del 2023

1 Introducción

Una de las operaciones más frecuentemente vistas es el factorial de un número. Sea en combinatoria contando permutaciones, en cálculo al expandir series de Taylor o en Teoría de Números analizando sus propiedades, esta operación aparece en todas partes. En este folleto, analizaremos a los factoriales bajo el microscopio de la teoría de números.

2 Fundamentos

Para un entero positivo n, denotamos por $n!$ a la expresión $n \cdot (n-1) \cdot (n-1) \cdots 2 \cdot 1$. También, definimos $0! := 1$. Algo importante de los factoriales, es que como son el producto de todos los enteros que son a lo sumo algún n, son divisibles entre todo entero que es a lo sumo n. Es decir, para todo $1 \leq k \leq n$,

$$k \mid n!.$$

Ejemplo 1

Demuestra que para todo entero positivo k, existen k enteros consecutivos ninguno de los cuales es primo.

Demostración. La clave es aprovecharnos de la alta divisibilidad de los factoriales. Si tenemos un $n \geq k$, sabemos que $n! + k$ es divisible entre k. Además, como claramente $n! + k > k$, sigue que debe ser compuesto. Entonces, tomamos los k enteros consecutivos

$$(k+1)! + 2, (k+1)! + 3, \dots, (k+1)! + k, (k+1)! + (k+1).$$

Como ya establecimos, todos estos son compuestos, por lo cual tenemos k enteros consecutivos, ninguno de los cuales es primo. ■

A veces nos interesa ver cuando un primo p divide a $n!$. Afortunadamente, esto es muy sencillo de comprobar:

Lema 1: Primos dividiendo a $n!$

Sea p un primo y n un entero positivos. Tenemos que $p \mid n!$ si y solo si $p \leq n$.

Demostración. Si $p \leq n$, entonces p es uno de los factores de $n!$, así que $p \mid n!$. Por otro lado, si $p \mid n!$, como p es primo sigue que p divide uno de $n, n-1, \dots, 2, 1$. Supongamos que k es uno de los factores al cual p divide. En tal caso, $p \leq k \leq n$, como queríamos demostrar. ■

Notemos que esto no es necesariamente cierto si para los números compuestos. Por ejemplo, $6 \mid 3!$ aunque $6 > 3$. Sin embargo, ¡hay un compuesto para el cual esto sí es cierto! Notemos que 4 no divide a $1!, 2!, 3!$. Como veremos luego, 4 es el único compuesto para el cual esto se cumple.

También es conveniente saber cual es la máxima potencia de un primo p que divide a $n!$. Introducimos un poco de notación:

Definición 1: Valoración $p-$ádica de un número

Sea p un primo y n un entero positivo. Denotamos por $\nu_p(n)$ al entero k tal que $p^k \mid n$ y $p^{k+1} \nmid n$. Es decir, $\nu_p(n)$ es el máximo exponente al que podemos elevar p tal que aún divida a n.

Algunos ejemplos: $\nu_3(6) = 1, \nu_2(8) = 3, \nu_7(98) = 2, \nu_5(23) = 0$.
Ejercicio 1. Demuestra que $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ y $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$.
Ejercicio 2. Demuestra que $\nu_p(a^n) = n \cdot \nu_p(a)$.

Regresando a factoriales, la siguiente fórmula gracias a Legendre nos dice cual es la máxima potencia de un primo dividiendo un factorial:

Teorema 1: Fórmula de Legendre

Sea p un primo y n un entero positivo. Entonces,

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

Demostración. Contamos cada vez que aparece una potencia de p en el producto. Notemos que hay $\left\lfloor \frac{n}{p} \right\rfloor$ enteros entre 1 y n divisibles entre p. Sumamos uno al exponente para cada uno de ellos. Luego, hay $\left\lfloor \frac{n}{p^2} \right\rfloor$ enteros divisibles entre p^2. Como ya contamos uno de los factores de p en la cuenta anterior, sumamos un solo factor más. Continuamos este proceso para cada potencia de p hasta que $p^k > n$, y vemos que

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

como deseábamos demostrar. ■

Esta fórmula es especialmente útil para el siguiente tipo de problemas:

Ejemplo 2

Determine cuantos ceros hay al final de 2023!.

Solución. La cantidad de ceros al final será dado por la máxima potencia de 10 que divida a 2023!. Para ello, necesitamos la máxima potencia de 2 y de 5 que dividan a 5! pues la menor de estas nos dará la máxima potencia de 10. Sin embargo, es claro que 2 divide a 2023! muchas más veces que 5, así que la respuesta será $\nu_5(2023!)$. Por la fórmula de Legendre,

$$\nu_5(2023!) = \left\lfloor \frac{2023}{5} \right\rfloor + \left\lfloor \frac{2023}{25} \right\rfloor + \left\lfloor \frac{2023}{125} \right\rfloor + \left\lfloor \frac{2023}{625} \right\rfloor + \left\lfloor \frac{2023}{3125} \right\rfloor + \dots = 404 + 80 + 16 + 3 + 0 + 0 + \dots = 503.$$

Por ende, 2023! termina en 503 ceros. ■

Un corolario de la fórmula de Legendre es la siguiente igualdad:

Lema 2: Fórmula de Legendre (2)

Sea $s_p(n)$ la suma de los dígitos de n cuando lo escribimos en base p. Entonces,

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Demostración. Sean $a_0, a_1, \ldots, a_k$ los enteros no-negativos menores a p tales que

$$n = a_k p^k + a_{k-1}p^{k-1} + \ldots + a_1 p + a_0.$$

En particular, $n = \overline{a_k a_{k-1} \ldots a_1 a_0}$ en base p. Por la fórmula de Legendre, vemos que

$$\nu_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \sum_{j=1}^{\infty} \left\lfloor a_k p^{k-j} + \ldots + a_1 p^{1-j} + a_0 p^{-j} \right\rfloor .$$

Agrupando términos con el mismo a_i, vemos que

$$\nu_p(n!) = \sum_{i=0}^{k} a_k (p^{k-1} + \ldots + p + 1) = \frac{1}{p-1} \sum_{i=0}^{k} a_k (p^k - 1).$$

Podemos escribir la expresión como

$$\nu_p(n!) = \frac{1}{p-1} \left(\sum_{i=0}^{k} a_k p^k - \sum_{i=0}^{k} a_k \right) = \frac{n - s_p(n)}{p-1},$$

tal como queríamos demostrar. ■

Ejercicio 3. Demuestra que $\nu_p(n!) < \frac{n}{p-1}$.

3 Wilson y $(n-1)!$

En nuestra discusión previa, demostramos que un primo p divide a $n!$ si y solo si $n \geq p$. En particular, esto significa que $p \nmid (p-1)!$. Sin embargo, es difícil creer que $(p-1)!$ no tendrá algún valor especial con respecto a p. Por ello, veamos p y $(p-1)!$ para algunos casos pequeños:

p	$(p-1)!$
2	1
3	2
5	24
7	720

Curiosamente, vemos que para estos ejemplos $p \mid (p-1)! + 1$. Escrito con aritmética modular, hemos descubierto el teorema de Wilson:

Teorema 2: Teorema de Wilson

Sea p un primo. Entonces,

$$(p-1)! \equiv -1 \pmod{p}$$

Demostración. Recordemos que todo residuo distinto de 0 tiene un inverso módulo p, pues este es primo. Ahora, si tenemos un residuo x, este es su propio inverso si y solo si $x^2 \equiv 1 \pmod{p}$. Esto es equivalente a $(x-1)(x+1) \equiv 0 \pmod{p}$, y como p es primo, esto significa que x sería o 1 o -1. Por ende, todo otro residuo tiene un inverso distinto a si mismo. Entonces, en el producto $(p-1)!$ podemos emparejar los factores que no son 1 ni $p-1$ en parejas de inversos. Estas parejas son $1 \pmod p$, así que

$$(p-1)! \equiv 1 \cdot 1 \cdots 1 \cdot (p-1) \equiv -1 \pmod p,$$

como deseábamos demostrar. ■

Ejercicio 4. Demuestra que $(p-2)! \equiv 1 \pmod p$.

Este análisis nos lleva a la pregunta: Para n entero positivo, ¿cuál es la relación entre n y $(n-1)!$? La respuesta es la siguiente:

Teorema 3: n **y** $(n-1)!$

Sea n un entero positivo. Entonces,

$$(n-1)! \equiv \begin{cases} -1 \pmod n & \text{si } n \text{ es primo} \\ 2 \pmod n & \text{si } n = 4 \\ 0 \pmod n & \text{de lo contrario} \end{cases}$$

Demostración. Cuando n es primo este es el Teorema de Wilson. Si $n = 1$, claramente $1 \mid 0!$. Ahora, tratamos el caso cuando n es compuesto. Como n es compuesto, existen enteros a y b tales que $n = ab$ y $1 < a, b < n$. En particular, a y b aparecen en el producto $(n-1)!$. Sin embargo, debemos tener cuidado, pues es posible que $a = b$. Si n no es de la forma p^2, con p primo, entonces podemos escoger a y b tales que sean distintos. En este caso, $n = ab \mid (n-1)!$, como queríamos demostrar. De lo contrario, $n = p^2$. En este caso, tendríamos que $n \mid (n-1)!$ si y solo si $(p^2-1) \geq 2p$. Esto sucede para todo $p > 2$, así que $n \mid (n-1)!$ en ese caso también. El único entero positivo con el que no hemos lideado es $n = 2^2 = 4$. En este caso, $(n-1)! = 6 \equiv 2 \pmod 4$ y esto termina nuestra clasificación. ■

4 Conclusión

Los factoriales son una operación muy común y llena de propiedades. Entenderlos nos permite conseguir un entendimiento más profundo de la teoría de números y nos da una herramienta más para resolver problemas.