Relación entre el exponente de p en n! y la expresión de n en base p.

El exponente m tal que $p^m \mid n! = 1 \cdot 2 \cdot 3 \cdots n$, pero p^{m+1} no, con p primo, es igual a la cantidad de múltiplos de p menores que n, más la cantidad de múltiplos de p^2 menores que n ... más la cantidad de múltiplos de p^k menores que n, siendo esta la mayor potencia de p que es menor que n.

Es decir,

$$m = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots = \sum_{r=1}^{k} \left\lfloor \frac{n}{p^r} \right\rfloor = \sum_{r=1}^{\infty} \left\lfloor \frac{n}{p^r} \right\rfloor$$

teniendo en cuenta que

$$\left\lfloor \frac{n}{p^r} \right\rfloor = 0 \text{ para } r > k = \left\lfloor \log_p n \right\rfloor .$$

Sea $n = a_k a_{k-1} \cdots a_1 a_0,\ 0 \le a_i < p$, la expresión en base p de n, y s la suma de los dígitos en tal expresión:

$$n = \sum_{i=0}^{k} a_i p^i, \qquad s = \sum_{i=0}^{k} a_i$$

Entonces,

$$\begin{aligned} \left\lfloor \frac{n}{p^r} \right\rfloor &= \left\lfloor \frac{a_0 + a_1 p + \cdots + a_{r-1} p^{r-1}}{p^r} + a_r + a_{r+1} p + \cdots + a_k p^{k-r} \right\rfloor \\ &= a_r + a_{r+1} p + \cdots + a_k p^{k-r} \end{aligned}$$

puesto que

$$\begin{aligned} a_0 + a_1 p + \cdots + a_{r-1} p^{r-1} &\le (p-1) + (p-1)p + \cdots + (p-1)p^{r-1} \\ &= (p-1)\frac{p^r - 1}{p-1} = p^r - 1 < p^r \end{aligned}$$

Entonces,

$$\begin{array}{rcl} \left\lfloor \frac{n}{p} \right\rfloor & = & a_1 + a_2 p + a_3 p^2 + \cdots + a_k p^{k-1} \\ \left\lfloor \frac{n}{p^2} \right\rfloor & = & a_2 + a_3 p + \cdots + a_k p^{k-2} \\ \left\lfloor \frac{n}{p^3} \right\rfloor & = & + a_3 + \cdots + a_k p^{k-3} \\ \cdots & = & \cdots \\ \left\lfloor \frac{n}{p^k} \right\rfloor & = & a_k \end{array}$$

Sumando,

$$m = a_1 + a_2(1+p) + a_3(1+p+p^2) + \cdots + a_k(1+p+p^2+\cdots+p^{k-1})$$

$$= \frac{a_1(p-1)}{(p-1)} + \frac{a_2(p^2-1)}{(p-1)} + \frac{a_3(p^3-1)}{(p-1)} + \cdots + \frac{a_k(p^k-1)}{(p-1)} \Rightarrow$$

$$(p-1)m = \left(a_0 + a_1 p + a_p^2 + \cdots + a_k p^k\right) - (a_0 + a_1 + a_2 + \cdots + a_k) = n - s \ \square$$

Se trata de una generalización de la demostración para $p = 2$ que puede verse en el *Item 1* del capítulo 1 del libro *Mathematical Gems II* de Ross Honsberger (Dolciani Mathematical Expositions No. 2, Mathematical Association of America).