Number Theory

Factorial Factors: The factorials: $n! = 1 \cdot 2 \cdot \cdots \cdot n = \prod_{k=1}^{n} k$, integer $n \geq 0$

We can find out factorial of an integer *n* using following recursive formula:

$0! = 1$

$n! = n(n-1)!$, for $n > 0$

Here are the first few values of the factorial function.

n	0	1	2	3	4	5	6	7	8	9	10
$n!$	0	1	2	6	24	120	720	5040	40320	362880	3628800

Because of it's exponential nature it's very difficult to find a closed form of factorial. To approximate $n!$ more accurately for large n we can use Stirling's formula:

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

We would like to determine, for any given prime p, the largest power of p that divides $n!$; that is we want the exponent of p in $n!$'s unique factorization. We denote this number by $\varepsilon_p(n!)$, and we start our investigations with the small case $p = 2$ and $n = 10$.

Find $e_2(10!)$

= 8

	1	2	3	4	5	6	7	8	9	10	Powers of 2
Divisible by 2		X		X		X		X		X	$5 = \lfloor 10/2 \rfloor$
Divisible by 4				X				X			$2 = \lfloor 10/4 \rfloor$
Divisible by 8								X			$1 = \lfloor 10/8 \rfloor$
Powers of 2	0	1	0	2	0	1	0	3	0	1	8

For general n this method gives, $\varepsilon_2(n!) = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \left\lfloor \frac{n}{8} \right\rfloor + \cdots = \sum_{k \geq 1} \left\lfloor \frac{n}{2^k} \right\rfloor$

This sum is actually finite, since the summand is zero when $2^k > n$. Therefore it has only $\lfloor \lg n \rfloor$ nonzero terms, and it's computationally quite easy. For instance, if n = 100,

$$\varepsilon_2(100!) = \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{4} \right\rfloor + \left\lfloor \frac{100}{8} \right\rfloor + \left\lfloor \frac{100}{16} \right\rfloor + \left\lfloor \frac{100}{32} \right\rfloor + \left\lfloor \frac{100}{64} \right\rfloor = 50 + 25 + 12 + 6 + 3 + 1 = 97$$

Let's look at the binary representation of all numbers to find out what's going on.

$100 = (1100100)_2 = 100$

$\lfloor 100/2 \rfloor = (110010)_2 = 50$

$\lfloor 100/4 \rfloor = (11001)_2 = 25$

$\lfloor 100/8 \rfloor = (1100)_2 = 12$

$\lfloor 100/16 \rfloor = (110)_2 = 6$

$\lfloor 100/32 \rfloor = (11)_2 = 3$

$\lfloor 100/64 \rfloor = (1)_2 = 1$

We merely drop the least significant bit from one term to get the next. The binary representation shows us how to derive another formula,

$\boxed{\varepsilon_2(n!) = n - v_2(n), \quad \text{where } v_2(n) \text{ is the number of 1's in the binary representation of } n.}$

Generalizing our findings to an arbitrary prime p, we have

$$\varepsilon_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots = \sum_{k \ge 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

We can find out the upper bound of $\varepsilon_p(n!)$ by simply removing the floor from the summand and then summing an infinite geometric progression.

Prove that ...

$$\begin{aligned}
\varepsilon_p(n!) \leqslant \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots &= \frac{n}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\
&= \frac{n}{p}\left(1 - \frac{1}{p}\right)^{-1} \qquad ;[\because \frac{1}{p} < 1] \\
&= \frac{n}{p}\left(\frac{p-1}{p}\right)^{-1} \\
&= \frac{n}{p}\left(\frac{p}{p-1}\right) \\
&= \frac{n}{p-1}
\end{aligned}$$

For example, when $p = 2$ and $n = 100$, this inequality says that $97 < 100$. Thus the upper bound 100 is not only correct but also close to the true value 97.

☺Good Luck☺