THE PRIME DECOMPOSITION OF $n!$

A. M. KASPRZYK

We shall prove the following result:

Theorem. *Let $n \in \mathbb{N}$ and let p be prime. Then the power of p in the prime decomposition of $n!$ is given by:*

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots .$$

The proof is not simple, and we shall approach it in small stages. For a long while it may seem that we're simply introducing more and more notation, whilst getting no nearer to proving the result. Have faith. Take your time and understand each step in turn – we get there in the end![1]

Remark. Note that the sum in the Theorem has only finitely many non-zero terms, since there exists some $\kappa \in \mathbb{N}$ such that $p^\kappa > n$, and so for any $r \geq \kappa$ we have that $n/p^r < 1$, i.e. $\lfloor n/p^r \rfloor = 0$.

Example. *First let's consider an example:* $12!$. *This is equal to:*

$$12! = 2 \cdot 3 \cdot 4 \cdot \ldots \cdot 12.$$

Thus, if we wish to calculate the prime decomposition of $12!$*, it seems sensible to proceed by calculating the prime decomposition of m for each $m \in \{2, 3, 4, \dots, 12\}$. We obtain:*

$$12! = (2^1)(3^1)(2^2)(5^1)(2^1 3^1)(7^1)(2^3)(3^2)(2^1 5^1)(11^1)(2^2 3^1).$$

The power of 2 *in the prime decomposition of* $12!$ *is given by* $1 + 2 + 1 + 3 + 1 + 2$*, the power of* 3 *is given by* $1 + 1 + 2 + 1$*, the power of* 5 *is* $1 + 1$*, and the powers of* 7 *and* 11 *are both* 1*. i.e.*

$$12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11.$$

[1] In the interests of clarity, I've perhaps been a little slap–dash over my handling of those cases where $p^0 = 1$ is the largest power of p dividing an integer m. In fact the proof proceeds in exactly the same fashion. Such technical details are, in my opinion, less important that understanding the ideas behind the proof.

Proof of the Theorem. Now consider any $n \in \mathbb{N}$. We are interested in determining the prime decomposition of $n!$. We adopt a similar strategy to the example above. We consider the prime factorisation of each $m \in \{2, 3, 4, \ldots, n\}$, and from this deduce the powers of each prime p.

Step 1. Let us fix a prime p. For convenience let $A := \{2, 3, 4, \ldots, n\}$. For each $m \in A$, let $k_m \in \mathbb{N}$ be the power of p occurring in the prime decomposition of m. i.e. $p^{k_m} \mid m$ but $p^{k_m+1} \nmid m$. Then the power of p in the prime decomposition of $n!$ is simply given by:

$$k_2 + k_3 + k_4 + \ldots + k_n = \sum_{m \in A} k_m.$$

Thus it would seem that the sensible approach is to calculate k_m for each $m \in A$.

Step 2. In fact we turn the problem on its head. Instead of calculating k_m for each $m \in A$, we fix some $k \in \mathbb{N}$ and ask "for how many $m \in A$ does $k_m = k$?". Let us write A_k for the collection of all such m:

$$A_k := \{m \in A \mid k_m = k\}.$$

Then each $m \in A$ will appear in exactly one A_k, namely A_{k_m}. We say that the A_k *partition* A.

For each $m \in A_k$ we have that $k_m = k$. Thus:

$$\sum_{m \in A_k} k_m = \sum_{m \in A_k} k = k \left|A_k\right|,$$

where $|A_k|$ denotes the number of elements in A_k. Since the A_k partition A, we see that:

$$\begin{aligned}
\sum_{m \in A} k_m &= \sum_{m \in A_1} k_m + \sum_{m \in A_2} k_m + \sum_{m \in A_3} k_m + \ldots \\
&= \sum_{k \in \mathbb{N}} \sum_{m \in A_k} k_m \\
&= \sum_{k \in \mathbb{N}} \sum_{m \in A_k} k \\
&= \sum_{k \in \mathbb{N}} k \left|A_k\right|.
\end{aligned}$$

Hence the power of p in the prime decomposition of $n!$ is given by:

$$\sum_{k \in \mathbb{N}} k \left|A_k\right|.$$

It remains to calculate $|A_k|$. With this aim in mind, we introduce some new notation.

Step 3. Let B_k be the set of all those $m \in A$ such that $p^k \mid m$. i.e.

$$B_k := \left\{m \in A \mid p^k \text{ divides } m\right\}.$$

Clearly if $p^{k+1} \mid m$ then $p^k \mid m$. Hence we have that if $m \in B_{k+1}$ then $m \in B_k$. We obtain:

$$B_1 \supseteq B_2 \supseteq B_3 \supseteq \dots.$$

If $m \in B_k$ but $m \notin B_{k+1}$ then $p^k \mid m$ but $p^{k+1} \nmid m$. Thus k is the largest power of p which divides m. Hence the power of p which occurs in the prime decomposition of m is k. Thus $m \in A_k$. Conversely if $m \in A_k$ then the largest power of p dividing m is k, and so we see that $m \in B_k$ but $m \notin B_{k+1}$. Hence:

$$A_k = B_k \setminus B_{k+1}.$$

Since $B_{k+1} \subseteq B_k$ we have that:

$$|B_k \setminus B_{k+1}| = |B_k| - |B_{k+1}|.$$

Thus:

$$|A_k| = |B_k| - |B_{k+1}|.$$

Hence the power of p in the prime decomposition of $n!$ is given by:

$$\begin{aligned}
\sum_{k\in\mathbb{N}} k\,|A_k| &= \sum_{k\in\mathbb{N}} k(|B_k| - |B_{k+1}|) \\
&= \sum_{k\in\mathbb{N}} k\,|B_k| - \sum_{k\in\mathbb{N}} k\,|B_{k+1}| \\
&= \sum_{k\in\mathbb{N}} k\,|B_k| - \sum_{k\in\mathbb{N}} (k-1)\,|B_k| \\
&= \sum_{k\in\mathbb{N}} (k-k+1)\,|B_k| \\
&= \sum_{k\in\mathbb{N}} |B_k|.
\end{aligned}$$

Step 4. The end is in sight! If we can find a way of calculating $|B_k|$ then we are done. Now $m \in A$ is an element of B_k if and only if $p^k \mid m$. i.e. there exists some $d \in \mathbb{N}$ such that $dp^k = m \leq n$. Hence we see that the elements of B_k are given by:

$$1p^k, 2p^k, 3p^k, \dots, cp^k,$$

where $c \in \mathbb{N}$ is the largest integer such that $cp^k \leq n$. In other words, c is the largest integer such that $c \leq n/p^k$. The notation for this is:

$$c = \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Clearly $|B_k| = c$, and so $|B_k| = \left\lfloor n/p^k \right\rfloor$. Putting all this together, we see that the power of p in the prime decomposition of $n!$ is given by:

$$\sum_{k \in \mathbb{N}} |B_k| = \sum_{k \in \mathbb{N}} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

□

Example. *Let us calculate the prime decomposition of* $18!$. *We need to consider each prime* $p \leq 18$ *in turn, and apply the Theorem. Thus:*

p	Sum	Total
2	$\lfloor 18/2 \rfloor + \lfloor 18/4 \rfloor + \lfloor 18/8 \rfloor + \lfloor 18/16 \rfloor$	$9 + 4 + 2 + 1 = 16$
3	$\lfloor 18/3 \rfloor + \lfloor 18/9 \rfloor$	$6 + 2 = 8$
5	$\lfloor 18/5 \rfloor$	3
7	$\lfloor 18/7 \rfloor$	2
11	$\lfloor 18/11 \rfloor$	1
13	$\lfloor 18/13 \rfloor$	1
17	$\lfloor 18/17 \rfloor$	1

Hence we have that:

$$18! = 2^{16} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17.$$