Highest power of a prime p dividing $N!$

How does one find the highest power of a prime p that divides $N!$ and other related products?

Related question: How many zeros are there at the end of $N!$?

This is being done to reduce abstract duplicates. See Coping with *abstract* duplicate questions. and List of Generalizations of Common Questions for more details.

(algebra-precalculus) (elementary-number-theory) (factorial) (faq)

asked May 5 '12 at 0:49

community wiki
user17762

5 Answers

Largest power of a prime dividing $N!$

In general, the highest power of a prime p dividing $N!$ is given by

$$s_p(N!) = \left\lfloor \frac{N}{p} \right\rfloor + \left\lfloor \frac{N}{p^2} \right\rfloor + \left\lfloor \frac{N}{p^3} \right\rfloor + \cdots$$

The first term appears since you want to count the number of terms less than N and are multiples of p and each of these contribute one p to $N!$. But then when you have multiples of p^2 you are not multiplying just one p but you are multiplying two of these primes p to the product. So you now count the number of multiple of p^2 less than N and add them. This is captured by the second term $\left\lfloor \frac{N}{p^2} \right\rfloor$. Repeat this to account for higher powers of p less than N.

Number of zeros at the end of $N!$

The number of zeros at the end of $N!$ is given by

$$\left\lfloor \frac{N}{5} \right\rfloor + \left\lfloor \frac{N}{5^2} \right\rfloor + \left\lfloor \frac{N}{5^3} \right\rfloor + \cdots$$

where $\left\lfloor \frac{x}{y} \right\rfloor$ is the greatest integer $\leq \frac{x}{y}$.

To make it clear, write $N!$ as a product of primes $N! = 2^{\alpha_2} 3^{\alpha_2} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}} \ldots$ where $\alpha_i \in \mathbb{N}$.

Note that $\alpha_5 < \alpha_2$ whenever $N \geq 2$. (Why?)

The number of zeros at the end of $N!$ is the highest power of 10 dividing $N!$

If 10^α divides $N!$ and since $10 = 2 \times 5$, $2^\alpha | N!$ and $5^\alpha | N!$. Further since $\alpha_5 < \alpha_2$, the highest power of 10 dividing $N!$ is the highest power of 5 dividing $N!$ which is α_5.

Note that there will be

1. A jump of 1 zero going from $(N-1)!$ to $N!$ if $5 \parallel N$
2. A jump of 2 zeroes going from $(N-1)!$ to $N!$ if $5^2 \parallel N$
3. A jump of 3 zeroes going from $(N-1)!$ to $N!$ if $5^3 \parallel N$ and in general
4. A jump of k zeroes going from $(N-1)!$ to $N!$ if $5^k \parallel N$

where $a \parallel b$ means a divides b and $\gcd\left(a, \frac{b}{a}\right) = 1$.

Largest power of a prime dividing other related products

In general, if we want to find the highest power of a prime p dividing numbers like $1 \times 3 \times 5 \times \cdots \times (2N-1)$, $P(N,r)$, $\binom{N}{r}$, the key is to write them in terms of factorials.

For instance,

$$1 \times 3 \times 5 \times \cdots \times (2N-1) = \frac{(2N)!}{2^N N!}.$$

Hence, the largest power of a prime, $p > 2$, dividing $1 \times 3 \times 5 \times \cdots \times (2N-1)$ is given by $s_p((2N)!) - s_p(N!)$, where $s_p(N!)$ is defined above. If $p = 2$, then the answer is $s_p((2N)!) - s_p(N!) - N$.

Similarly,

$$P(N,r) = \frac{N!}{(N-r)!}.$$

Hence, the largest power of a prime, dividing $P(N,r)$ is given by $s_p(N!) - s_p((N-r)!)$, where $s_p(N!)$ is defined above.

Similarly,

$$C(N,r) = \binom{N}{r} = \frac{N!}{r!(N-r)!}.$$

Hence, the largest power of a prime, dividing $C(N,r)$ is given by

$$s_p(N!) - s_p(r!) - s_p((N-r)!)$$

where $s_p(N!)$ is defined above.

edited Mar 29 '15 at 15:20

community wiki
6 revs, 3 users 86%
user17762

Yes you are right. I have deleted the corresponding part in the post. – user17762 May 5 '12 at 1:19

In my example, I meant highest power of 12 that divides $3!$. If m is square-free, then indeed the largest prime that divides m is the obstruction. – André Nicolas May 5 '12 at 1:32

@AndréNicolas Yes I recognized it. Thanks. For instance, in the highest power of 24 dividing $10!$ the prime 2 acts as the bottleneck since 2^3 divides 24 whereas only 3^1 divides 24 and since 10 is square-free it works. Is there a generic formula known for composite m? – user17762 May 5 '12 at 1:36

One trick that makes computations easier is

$$\left\lfloor \frac{N}{p^{n+1}} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{N}{p^n} \right\rfloor}{p} \right\rfloor$$

– steven gregory Jun 1 '16 at 8:26

---

de Polignac's formula named after Alphonse de Polignac, gives the prime decomposition of the factorial $n!$.

answered May 5 '12 at 4:38

community wiki
Michael Hardy

3 Sometimes the formula is also attributed to Legendre. – J. M. isn't a mathematician May 5 '12 at 4:46

For something completely different, see page 114 of Concrete Mathematics by Graham, Knuth, Patashnik. The highest power of a prime p dividing $n!$ is n minus the sum of the integer digits of n in base p, all divided by $p-1$. In *Mathematica* you would write:

```
(n-Total[IntegerDigits[n,p]])/(p-1)
```

Hence, the number of trailing zeros of $n!$ is

```
(n-Total[IntegerDigits[n,5]])/4
```

I've found this method to be **much** faster than the sum of Floor functions...

answered Nov 5 '12 at 1:04

community wiki
KennyColnago

For a number n, define $\Lambda(n) = \log p$ if $n = p^k$ and zero elsewhen.

Note that $\log n = \sum_{d|n} \Lambda(d)$. If $N = n!$, then

$$\log N = \sum_{k=1}^{n} \log k = \sum_{k=1}^{n} \sum_{d|k} \Lambda(d) = \sum_{d=1}^{n} \Lambda(d) \left\lfloor \frac{n}{d} \right\rfloor$$

Since $\Lambda(d)$ is nonzero precisely when d is a power of a prime and in such case it equals $\log p$, the last sum equals

$$\sum_{p} \sum_{k \geqslant 1} \log p \left\lfloor \frac{n}{p^k} \right\rfloor$$

and this gives

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

If you write n is base p, say $n = a_0 + a_1 p + \cdots + a_k p^k$, the above gives that

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

where $s(n) = a_0 + \cdots + a_k$.

answered Jan 9 '15 at 20:13 community wiki Pedro Tamaroff

Very nice proof with using von Mangoldt function! +1 – RFZ Jun 9 '16 at 11:08

Define $e_p(n) = s_p(n!)$, as Marvis is using s_p for the highest exponent function...

We get

$$e_p(n) = s_p(n!) = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor$$

I thought I would prove this by mathematical induction. We need, for any positive integers m, n,

LEMMA:

(A) If $n + 1 \equiv 0 \pmod{m}$, then

$$\left\lfloor \frac{n+1}{m} \right\rfloor = 1 + \left\lfloor \frac{n}{m} \right\rfloor$$

(B) If $n + 1 \not\equiv 0 \pmod{m}$, then

$$\left\lfloor \frac{n+1}{m} \right\rfloor = \left\lfloor \frac{n}{m} \right\rfloor$$

For $n < p$, we know that p does not divide $n!$ so that $e_p(n) = s_p(n!)$ is 0. But all the $\left\lfloor \frac{n}{p^i} \right\rfloor$ are 0 as well. So the base cases of the induction is true.

Now for induction, increasing n by 1. If $n + 1$ is not divisible by p, then $e_p(n + 1) = e_p(n)$, while part (A) of the Lemma says that the sum does not change.

If $n + 1$ is divisible by p, let $s_p(n + 1) = k$. That is, there is some number $c \neq 0 \pmod{p}$ such that $n + 1 = cp^k$. From the Lemma, part (B), all the $\left\lfloor \frac{n}{p^i} \right\rfloor$ increase by 1 for $i \leq k$, but stay the same for $i > k$. So the sum increases by exactly k. But, of course, $e_p(n + 1) = s_p((n + 1)!) = s_p(n!) + s_p(n + 1) = e_p(n) + k$. So both sides of the middle equation increase by the same $s_p(n + 1) = k$, completing the proof by induction.

Note that it is not necessary to have n divisible by p to get nonzero $e_p(n)$. All that is necessary is that $n \geq p$, because we are not factoring n, we are factoring $n!$

answered Nov 3 '12 at 19:03 community wiki Will Jagy