Prime Factoring The Factorial of an Integer

by

John Kennedy
Mathematics Department
Santa Monica College
1900 Pico Blvd.
Santa Monica, CA 90405

jrkennedy6@gmail.com

Except for this comment explaining that it is blank for some deliberate reason, this page is intentionally blank!

Finding the Multiplicities of the Prime Factors of n!

The purpose of this paper is to explain an algorithm for computing the prime factorization of the integer $n!$. This presupposes a knowledge about how to find the prime factors of n. But since $n!$ only has prime factors that are primes less than or equal to n, we need only consider relatively small primes even when $n!$ is extremely large. Every prime factor of n is also a prime factor of $n!$, but usually with a higher multiplicity. Except for the trivial case $n = 2$, $n!$ always has additional prime factors that n doesn't have. Finding the prime factors of $n!$ leads to an efficient technique on a small machine to compute exact values for permutations and combinations. Before giving the actual steps in the algorithm we first present examples which motivate the relevant theoretical results which are also given before the program code.

Example 1 Find $C(100, 50)$, the number of combinations of 100 elements chosen 50 at a time.

Using the standard formula we can theoretically compute that

$$C(100, 50) = \frac{100!}{50! \cdot 50!} = \frac{100 \cdot 99 \cdot 98 \cdots 52 \cdot 51}{50!}$$

Canceling 50! into 100! seems to simplify a lot of the work, but the problem remains to reduce the resulting fraction which contains another 50! in its denominator. ∎

The most efficient way to compute $\dfrac{100!}{50! \cdot 50!}$ is to prime factor the three factorial numbers and then reduce, not by partially canceling factorials, but by applying the subtraction rule for exponents with the multiplicities of the prime factors. The number 100! is 158 digits long and even the number 50! is 65 digits long, but the largest prime involved in the computations for this example is only 97 since this is the largest prime factor of the numerator 100!. The last part of the calculation would require a multiple precision multiplication routine to multiply out the surviving prime powers. While this cannot be done on a standard 10-digit scientific calculator, it can be done with almost any programmable calculator, even one with somewhat limited memory.

Theorem 1 Let n denote a positive integer, $n > 1$, and let p be such that $1 < p \leq n$. Then IntegerPart$\left(\dfrac{n}{p}\right)$ is the number of integer multiples of p between 1 and n inclusive.

Proof: By the division algorithm there exists a quotient q and a remainder r such that

$$n = q \cdot p + r \text{ where } q \geq 0 \text{ and } 0 \leq r < p.$$

Since $p > 1$, the multiples of p are equally spaced points or marks on a number line, where $1 \cdot p$ lies somewhere to the right of 1. p need not be prime, nor even an integer, although in the applications which follow p will be a prime integer. See figure 1 on the next page.

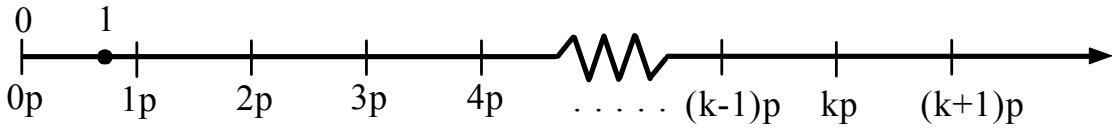

Figure 1. A number line showing the multiples of p as equally spaced points.

Since $n \geq p$, n lies to the right of the multiple $1 \cdot p$. n must lie between two successive multiples of p, or n is an exact multiple of p. In the latter case we let $r = 0$ and we let q denote the exact multiple of p. In the first case we let $q \cdot p$ and $(q + 1) \cdot p$ denote the two successive multiples of p between which n lies. See figure 2 below.

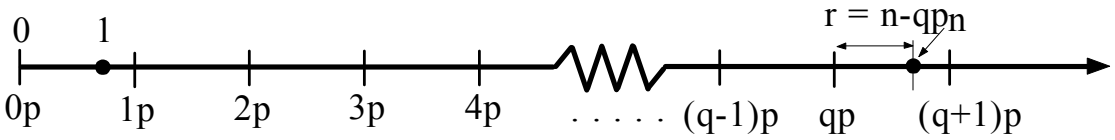

Figure 2. A number line showing the remainder distance up from a multiple of p.

Then we choose $r = n - q \cdot p$ and we can easily conclude that $0 \leq r < p$ in both cases. The distance between two successive marks is at most p. Each next mark is p units away from the previous mark. Note that $q \geq 1$. Finally,

$$\text{IntegerPart}\left(\frac{n}{p}\right) = \text{IntegerPart}\left(\frac{q \cdot p + r}{p}\right) = \text{IntegerPart}\left(\frac{q \cdot p}{p} + \frac{r}{p}\right) =$$

$$\text{IntegerPart}\left(q + \frac{r}{p}\right) = q$$

But q counts the number of multiples of p between 1 and n. ■ **Q.E.D.** ■

Example 2 Consider the number $38! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \cdot 18 \cdot 19 \cdot 20 \cdot 21 \cdot 22 \cdot 23 \cdot 234 \cdot 25 \cdot 26 \cdot 27 \cdot 28 \cdot 29 \cdot 30 \cdot 31 \cdot 32 \cdot 33 \cdot 34 \cdot 35 \cdot 36 \cdot 37 \cdot 38$

The problem is to find the largest power of 3 that is a factor of 38!.

To do this, we note that only the multiples of 3 that are less than 38 contribute. Thus we consider the string of factors

$$(3) \cdot (6) \cdot (9) \cdot (12) \cdot (15) \cdot (18) \cdot (21) \cdot (24) \cdot (27) \cdot (30) \cdot (33) \cdot (36)$$

There are twelve multiples of 3 that are less than 38. We rearrange the above product before writing all the 3's as the first factor.

$$(3 \cdot 1)(3 \cdot 2)(3 \cdot 3)(3 \cdot 4)(3 \cdot 5)(3 \cdot 6)(3 \cdot 7)(3 \cdot 8)(3 \cdot 9)(3 \cdot 10)(3 \cdot 11)(3 \cdot 12)$$

$$= 3^{12} \cdot (1) \cdot (2) \cdot (3) \cdot (4) \cdot (5) \cdot (6) \cdot (7) \cdot (8) \cdot (9) \cdot (10) \cdot (11) \cdot (12)$$

Then we extract from the product only those values that contribute powers of 3. We only deal with multiples of 3 in rearranging the product.

$$3^{12} \cdot (3) \cdot (6) \cdot (9) \cdot (12)$$

$$= 3^{12} \cdot (3 \cdot 1)(3 \cdot 2)(3 \cdot 3)(3 \cdot 4) \qquad \text{rearrange}$$

$$= 3^{12} \cdot 3^4 \cdot (1) \cdot (2) \cdot (3) \cdot (4) \qquad \text{re-group}$$

Lastly we see only one more multiple of 3 remains. So we continue to extract only those numbers that contribute 3 as a factor.

$$3^{12} \cdot 3^4 \cdot 3^1 = 3^{17}$$

We conclude that 3^{17} is the largest power of 3 that is a factor of 38!. ∎

More Comments About the Examples

The powers of 3 that are less than or equal to 38 are 3^1, 3^2, and 3^3. There were 12 multiples of 3 less than 38, namely 3,6,9,12,15,18,21,24,27,30,33, and 36. There were fewer multiples of $9 = 3^2$ less than 38: namely 9,18,27, and 36. But each of these already appeared in the above list of multiples of 3. There were even fewer multiples of $27 = 3^3$ less than 38: namely only 27. But 27 already appeared in the first two lists of multiples of 3^1 and 3^2.

The last multiple of 3^1 was the same as the last multiple of 3^2. Both of these multiples were the number 36. But the last (and only) multiple of 3^3 was less than the last multiple of 3^2. $27 < 36$.

Applying the same technique on each of the 12 distinct primes that precede 38 we can show that:

$$38! = 2^{35} \cdot 3^{17} \cdot 5^8 \cdot 7^5 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23^1 \cdot 29^1 \cdot 31^1 \cdot 37^1$$

Also, from Example 1 we can show that

$$50! = 2^{47} \cdot 3^{22} \cdot 5^{12} \cdot 7^8 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29^1 \cdot 31^1 \cdot 37^1 \cdot 41^1 \cdot 43^1 \cdot 47^1$$

$$100! = 2^{97} \cdot 3^{48} \cdot 5^{24} \cdot 7^{16} \cdot 11^9 \cdot 13^7 \cdot 17^5 \cdot 19^5 \cdot 23^4 \cdot 29^3 \cdot 31^3 \cdot 37^2 \cdot 41^2 \cdot 43^2 \cdot 47^2 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97$$

Now we can easily derive the reduction of the fraction $\frac{100!}{50! \cdot 50!}$, even by hand. Double the $50!$ exponents and subtract from the $100!$ exponents.

$$C(100,50) = 2^3 \cdot 3^4 \cdot 11^1 \cdot 13^1 \cdot 17^1 \cdot 19^1 \cdot 29^1 \cdot 31^1 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97$$

Using a multiple precision multiplication program we can compute this product which is the following 30-digit number. This number appears far down in Pascal's Triangle.

$$C(100,50) = 100{,}891{,}344{,}545{,}564{,}193{,}334{,}812{,}497{,}256$$

Theorem 2 Let n denote any positive integer. Let p be any prime where $p \leq n$. If p is a prime factor of $n!$ then its multiplicity is given by

$$\sum_{k>0} \text{IntegerPart}\left(\frac{n}{p^k}\right)$$

Proof: For each k we need to compute how many times p^k appears in the list of numbers between 1 and n. By Theorem 1, while $p^k \leq n$, each such appearance contributes

$$\text{IntegerPart}\left(\frac{n}{p^k}\right)$$

to the final power of p that is part of the factorization of $n!$ ■ **Q.E.D.** ■

Looking back at **Example 2** we can see that for $p = 3$ and $k = 1,2,3$ we computed the multiplicity of 3 as a prime factor of $38!$ by computing

$$\text{IntegerPart}\left(\frac{38}{3^1}\right) + \text{IntegerPart}\left(\frac{38}{3^2}\right) + \text{IntegerPart}\left(\frac{38}{3^3}\right)$$

$$= 12 + 4 + 1 = 17$$

When $k = 4$, we could stop adding $\text{IntegerPart}\left(\frac{38}{3^k}\right)$ because once this quantity is 0 for a given integer k, it will be 0 for all higher values of k.

The next theorem shows that we can compute $\sum_{k>0} \text{IntegerPart}\left(\frac{n}{p^k}\right)$ recursively as a function of k and this is the key to an efficient algorithm to compute the prime factorization of $n!$.

Theorem 3 Let n denote a positive integer, $n > 1$, and let p be such that $1 < p \leq n$. Let $k > 1$ denote any positive integer where $p^{k+1} \leq n$. Then,

$$\text{IntegerPart}\left(\frac{n}{p^{k+1}}\right) = \text{IntegerPart}\left(\frac{\text{IntegerPart}\left(\frac{n}{p^k}\right)}{p}\right)$$

Proof: First note that every multiple of p^{k+1} is also a multiple of p^k. The number of multiples of p^{k+1} less than or equal to n, if anything, is smaller than the number of multiples of p^k that are less than or equal to n. The last multiple of p^k that is less than or equal to n, if anything, is larger than the last multiple of p^{k+1} that is less than or equal to n. If $p^{k+1} > n$, this theorem is still true, but then it says $0 = 0$. So in practice we assume $p^{k+1} \leq n$.

Let $r = \text{IntegerPart}\left(\frac{n}{p^k}\right) \cdot p^k$ and $s = \text{IntegerPart}\left(\frac{n}{p^{k+1}}\right) \cdot p^{k+1}$ Then $r \geq s$. There exists an integer j such that $s + j = r$, where $0 \leq j < p^{k+1}$. That $j < p^{k+1}$ is because s is the last multiple of p^{k+1} that is less than or equal to n. This inequality implies that $\frac{j}{p^{k+1}} < 1$.

Finally,

$$r = s + j$$

$$\text{IntegerPart}\left(\frac{n}{p^k}\right) \cdot p^k = \text{IntegerPart}\left(\frac{n}{p^{k+1}}\right) \cdot p^{k+1} + j$$

Now divide by p^{k+1} on both sides of the equation.

$$\frac{\text{IntegerPart}\left(\frac{n}{p^k}\right)}{p} = \text{IntegerPart}\left(\frac{n}{p^{k+1}}\right) + \frac{j}{p^{k+1}}$$

$$\text{IntegerPart}\left(\frac{\text{IntegerPart}\left(\frac{n}{p^k}\right)}{p}\right) = \text{IntegerPart}\left(\frac{n}{p^{k+1}}\right)$$

■ **Q.E.D.** ■

An Efficient Algorithm To Compute Multiplicities

The following is a Pascal language code fragment of a procedure that computes and returns the multiplicity of a prime factor of the factorial of an integer. The function INT computes the integer part of a number.

```
procedure GetMultiplicity(     OriginalInteger : longint;
                               PrimeDivisor    : longint;
                           var Multiplicity    : longint);
var  ScratchInteger : longint;
begin
   ScratchInteger := OriginalInteger;
   Multiplicity := 0;
   repeat
      ScratchInteger := INT(ScratchInteger/PrimeDivisor);
      inc(Multiplicity, ScratchInteger)
   until ScratchInteger=0
end;  {procedure GetMultiplicity}
```

When the above procedure is called with the parameters GetMultiplicity$(38, 3, M)$ the following table shows the progression of values through the main repeat-until loop. Compare with the numbers generated in **Example 2**.

ScratchInteger	**Multiplicity**
38	$M = 0$
$12 = \text{INT}(\frac{38}{3})$	$M = 12$
$4 = \text{INT}(\frac{12}{3})$	$M = 16 = 12 + 4$
$1 = \text{INT}(\frac{4}{3})$	$M = 17 = 16 + 1$
$0 = \text{INT}(\frac{1}{3})$	$M = 17$=17+0

the returned value of $M = 17$

Our last theorem gives the expression which yields the entire prime factorization of $n!$. This expression may be of intellectual curiosity only, but it is a direct consequence of **Theorem 2**.

Theorem 4 Let n denote any positive integer.

$$n! \;=\; \prod_{\substack{p \le n \\ p \text{ prime}}} p^{\left[\sum_{k>0} \text{IntegerPart}\left(\frac{n}{p^k}\right)\right]}$$

Proof: Apply **Theorem 2** to each of the primes less than or equal to n. ■ **Q.E.D.** ■