janmr blog

Prime Factors of Factorial Numbers

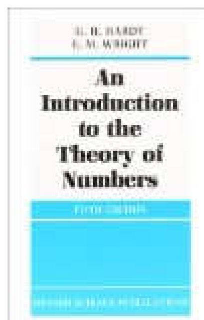
October 30, 2010

prime-numbers **factorials**

Factorial numbers, $n! = 1 \cdot 2 \cdots n$, grow very fast with n. In fact, $n! \sim \sqrt{2\pi n}(n/e)^n$ according to Stirling's approximation. The prime factors of a factorial number, however, are all relatively small, and the complete factorization of $n!$ is quite easy to obtain.

We will make use of the following fundamental theorem:

> $p \mid ab$ for a prime p, then $p \mid a$ or $p \mid b$.



(Here, $p \mid a$ means that p divides a.) This is called Euclid's First Theorem or Euclid's Lemma. For most, it is intuitively clear, but a proof can be found in, e.g., Hardy and Wright: An Introduction to the Theory of Numbers.

An application of this theorem to factorial numbers is that if a prime p is a divisor of $n!$ then p must be a divisor of at least one of the numbers $1, 2, \ldots, n$. This immediately implies

> Every prime factor of $n!$ is less than or equal to n.

Conversely, every prime number between 2 and n must be a prime factor of $n!$.

Let us introduce the notation $d_a(b)$ as the number of times a divides into b. Put more precisely, $d_a(b) = k$ if and only if b/a^k is an integer while b/a^{k+1} is not.

We now seek to determine $d_p(n!)$ for all primes $p \leq n$. From Euclid's First Theorem and the Fundamental Theorem of Arithmetic follows:

$$d_p(n!) = d_p(1) + d_p(2) + \cdots + d_p(n)$$

The trick here is not to consider the right-hand side term by term, but rather as a whole. Let us take

$$42! = 1405006117752879898543142606244511569936384000000000$$

and $p = 3$ as an example. How many of the numbers 1, 2, …, 42 are divisible by 3? Exactly $\lfloor 42/3 \rfloor = 14$ of them. But this is not the total count, because some of them are divisible by 3 multiple times. So how many are divisible by 3^2? $\lfloor 42/3^2 \rfloor = 4$ of them. Similarly, $\lfloor 42/3^3 \rfloor = 1$. And $\lfloor 42/3^4 \rfloor = \lfloor 42/3^5 \rfloor = \ldots = 0$. So we have

$$d_3(42!) = 14 + 4 + 1 = 19.$$

This procedure is easily generalized and we have

$$d_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\lfloor \log_p(n) \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor. \tag{1}$$

This identity was found by the french mathematician Adrien-Marie Legendre (see also Aigner and Ziegler: Proofs from The Book, page 8, where it is called Legendre's Theorem).

Doing this for all primes in our example, we get

$$42! = 2^{39} \cdot 3^{19} \cdot 5^9 \cdot 7^6 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41.$$

Notice how the exponents do not increase as the prime numbers increase. This is true in general. Assume that p and q are both primes and $p < q$. Then $\log_p(n) \geq \log_q(n)$ and $n/p^k \geq n/q^k$ for all positive integers k. Using this in equation (1) we get

About

A blog about mathematics and computer programming by Jan Marthedal Rasmussen.

Links

- All posts
- Twitter profile
- GitHub profile
- Subscribe in a reader

$$d_p(n!) \geq d_q(n!) \text{ for primes } p, q \text{ with } p < q \tag{2}$$

and thus

$$d_2(n!) \geq d_3(n!) \geq d_5(n!) \geq d_7(n!) \geq d_{11}(n!) \geq \dots$$

What about $d_k(n!)$ for composite numbers k? Given the factorization of both $n!$ and k, this is easy to compute. But if, e.g., the multiplicity of all prime factors of k are the same, then the relation (2) can be used. Consider $d_{10}(m)$ for a positive integer m. Since $10 = 2 \cdot 5$ then

$$d_{10}(m) = \min\{d_2(m), d_5(m)\}.$$

But if $m = n!$ then we can use (2) and we have

$$d_{10}(n!) = d_5(n!).$$

For instance,

$$d_{10}(42!) = d_5(42!) = \lfloor 42/5 \rfloor + \lfloor 42/5^2 \rfloor = 8 + 1 = 9,$$

so there are 9 trailing zeros in the decimal representation of 42!.

« Computing the Integer Binary Logarithm Where Did pi Come From? »