

# Project Euler: Problem 3 Personal Comments

Nathan Marianovsky

## FUNDAMENTAL THEOREM OF ARITHMETIC

For this question the only tool necessary is the prime factorization of any given natural number. To understand where the prime factorization comes from take a couple of numbers and reduce them down to a multiplication of their simplest terms:

$$45 = 1 \times 3^2 \times 5$$

$$12 = 1 \times 2^2 \times 3$$

$$31 = 1 \times 31$$

$$32 = 1 \times 2^5$$

Any number that behaves like 31 where its only factors are one and itself is known as a *prime* number. Prime numbers are the building blocks of all other numbers, though to do this day there is still no way to generate all of the primes numbers without checking by brute force. Notice the important aspect of the examples above though, each factorization consists purely of prime numbers. This is no coincidence since primes numbers are not divisible by anything but itself and one. This breakdown into a product of distinct prime numbers is what is known as the **Fundamental Theorem of Arithmetic**. We should consider two things now. How do we know if a factorization exists for every natural number and whether it is unique? First consider this proof for the existence of a factorization that consists strictly of prime numbers:

*Proof.* Consider a proof by induction. First we assume that every natural number can be written as a product of distinct prime numbers. For the base case we consider  $n = 2$  which is a prime number and meets the condition. Now for the general case take any natural number  $n$ . If  $n$  is prime the condition is met right away. On the other hand what if  $n$  is not prime? In this case there must exist numbers  $x$  and  $y$  such that  $n = xy$  where  $1 < x \leq y < n$ . Now according to the induction hypothesis  $x = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots p_n^{m_n}$  and  $y = q_1^{k_1} q_2^{k_2} q_3^{k_3} \dots q_l^{k_l}$  are products of distinct prime factors up to a multiplicity. With this  $n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots p_n^{m_n} q_1^{k_1} q_2^{k_2} q_3^{k_3} \dots q_l^{k_l}$  which is a product of prime numbers. ■

With existence taken care of lets now prove the uniqueness of the factorization:

*Proof.* Consider a proof by contradiction. Assume for any natural number  $n$  there are two factorizations that are not the same:

$$n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots p_n^{m_n} = q_1^{k_1} q_2^{k_2} q_3^{k_3} \dots q_l^{k_l}$$

We now have to show that each  $p_i$  is equal to some  $q_j$  with equal multiplicity and  $n = l$ . Take the above and divide through by  $p_1^{m_1}$ :

$$\frac{n}{p_1^{m_1}} = p_2^{m_2} p_3^{m_3} \dots p_n^{m_n} = \frac{q_1^{k_1} q_2^{k_2} q_3^{k_3} \dots q_l^{k_l}}{p_1^{m_1}}$$

We know that each  $p_i$  up to multiplicity will divide  $n$  giving back a natural number. If this is true, then this same factor must also divide the other factorization. Now if this prime divides the prime factorization it means that one of the  $q_j$  up to multiplicity must be equal to this  $p_i$ . For simplicity lets say that  $p_1 = q_1$  giving:

$$\frac{n}{p_1^{m_1}} = p_2^{m_2} p_3^{m_3} \dots p_n^{m_n} = q_1^{k_1-m_1} q_2^{k_2} q_3^{k_3} \dots q_l^{k_l}$$

Repeating this process for all the  $p$ 's gives:

$$1 = q_1^{k_1-m_1} q_2^{k_2-m_2} q_3^{k_3-m_3} \dots q_l^{k_l-m_n}$$

For the above to be true either all of the  $q_j$  are 1 simultaneously or the power of each  $q_j$  is 0. Since the first suggestion is impossible, the latter must be satisfied giving the condition  $k_i = m_j$  which states that all powers

are equal. At the same time notice that  $n = l$  because if there were more  $q$ 's than  $p$ 's then the right side would contain another prime factor which would make it not equal to 1 giving a contradiction. To conclude the proof we just have to consider the fact that we chose each  $p_i$  to divide  $q_j$  where  $i = j$ . This does not have to be true. This essentially states that any prime factorization is unique up to order. ■