1 Problem Statement

If we list all the natural numbers below 10 that are multiples of 3 or 5, we get 3, 5, 6 and 9. The sum of these multiples is 23.

Find the sum of all the multiples of 3 or 5 below 1000.

2 Solution

To sum up all the multiples of any pair of numbers below some finite threshold, we sum all the multiples of the first number, then sum all the multiples of the second number, and subtract all the repeated multiples. The repeated multiples are simply the multiples of both. As discussed below, the multiples of both are actually just the multiples of the least common multiple (LCM). In the case of two prime numbers, the LCM is the product of the two primes. In the case of non-prime numbers, the LCM is the product of the all of the unique primes that compose the two numbers factorizations. As an example, the LCM of 100 and 150:

$$100 = 2^2 5^2$$
$$150 = 2^1 3^1 5^2$$

And thus, we have two factors of 2, 2 factors of 5, and one factor of 3 or 300. Finally to actually get the sums, we use Gauss's formula:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

which is proven below.

In this case, we sum up all the numbers divisible by 3:

$$3 + 6 + ... + 996 + 999 = 3(1 + 2 + ... + 332 + 333) = 3 \sum_{i=1}^{333} i = 3 \frac{333(334)}{2} = 166833$$

And all the numbers divisible by 5:

$$5 + 10 + ... + 995 + 1000 = 5(1 + 2 + ... + 199 + 200) = 5 \sum_{i=1}^{200} i = 5 \frac{200(201)}{2} = 100500$$

And subtract all the numbers divisible by both, i.e. the multiples of 15:

$$15 + 30 + ... + 975 + 990 = 15(1 + 2 + ... + 66) = 15 \sum_{i=1}^{66} i = 15 \frac{66(67)}{2} = 33165$$

Thus the final solution is:

$$234168$$

3 Proofs

3.1 Gauss's Sum Formula

Gauss's sum formula:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

and sum formula's more generally are typically proven using a method called Proof by Induction. The idea is as follows: if we assume the formula holds true for case n and we can show that this assumption implies that it also holds for the $n+1$ case, then as long as we have a base case from which to build the formula holds generally. The idea is that the base case provides a starting point and then we just add one to n until we get to the case of interest. The sums are of a finite number of numbers, so if we apply going from case n to $n+1$ we will get there eventually.

To see what I mean in action, I will now prove Gauss's formula through induction. Thus, assume:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

But then:

$$\sum_{i=1}^{n+1} i = 1 + 2 + ... + n + (n+1) = \left(\sum_{i=1}^{n} i\right) + (n+1)$$
$$= \frac{n(n+1)}{2} + (n+1) = (n+1)\left(\frac{n}{2} + 1\right) = \frac{(n+1)(n+2)}{2}$$

And we've derived the same formula for the $n+1$ case by apply the formula for the n case. The final piece is to have a base case. Consider then $n = 1$:

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2} = 1$$

Thus the formula holds for the base case of $n = 1$. We can then use the above and this fact to build the case for $n = 2$, and then the case for $n = 3$, and so on.

3.2 Divisibility and the Least Common Multiple

Fundamental to this solution is that we can enumerate all the multiples of the two numbers and avoid double counting multiples of both by subtracting off the multiples of the least common multiple. Why does this work? I'm borrowing some of these proofs and ideas from I.N. Herstein's book Abstract Algebra, Third Edition. To begin defining everything, we must first state Euclid's Algorithm: if m and n are integers with $n > 0$, then there exist q and r, with $0 \leq r < n$, such that

$m = qn + r$. This represents a number as it's quotient, q and it's remainder r. A couple of examples:

$$\begin{aligned} m = 16n = 5 &\implies q = 3r = 1 \\ m = 5n = 16 &\implies q = 0r = 5 \\ m = -5n = 16 &\implies q = -1r = 11 \end{aligned}$$

I provide a proof by construction to show why this is so. If $m = 0$, for any $n > 0$, we find $q = 0$ and $r = 0$. If $m > 0$, we start with $q = 0$ and evaluate $m - qn = r$. Now, we have three cases, $0 \leq r < n$, $r < 0$, or $r \geq n$. In the first case, we've found the r from the theorem. The second case, at $q = 0$, requires $m < 0$, a contradiction. Thus, the only remaining case of interest is $r \geq n$. Thus, increment q by 1 to $q' = q + 1$, and see that $r' = m - q'n = m - (q + 1)n = m - qn - n = r - n$. Thus, since $r \geq n$, either $r' = 0$, giving us the r of interest or $r' > n$. If $r' > n$, increment q' again, repeating until completion. Because m is a single finite integer, we only need to perform this a finite number of steps and thus we've constructed q and r for $m > 0$.

For $m < 0$, we start with $q = -1$. In this case, $r = m - qn$. We have three cases, $0 \leq r < n$, $r \geq n$, or $r < 0$. In the first case, we've found the r from the theorem. In the second case, at $q = -1$, $r = m - qn = m + n > n \implies m > 0$, a contradiction. Thus, the only case of interest is $r < 0$. If $r < 0$, we decrement q to $q' = q - 1$, and find $r' = m - q'n = m - (q - 1)n = m - qn + n = r + n$. Because $r < 0$, this means $r' < n$. Thus, we see either $0 \leq r' < n$ or $r' < 0$. Once again, the first case completes the construction, and in the second case we decrement q. Because m is a single finite integer, we only need to perform this a finite number of steps and thus we've constructed q and r for $m > 0$. (There's probably a more elegant way to prove this, but this way shows how quotient and remainder get constructed more generally, so I like it).

And from Euclid's Algorithm, we can define divisibility: We say a number $n \neq 0$ is a divisor of m if for some integer c we can write $m = cn$ (i.e. $q = c$ and $r = 0$). Another way to think of this is that m is a multiple of n. We can also define prime as any number, p whose only divisors are 1 and p. We can also say that two numbers are co-prime if their sets of divisors share only 1. Finally, we can define the least common multiple of $n_1 > 0$ and $n_2 > 0$ to be the smallest number $m > 0$ such that n_1 and n_2 are both divisors. How does this help us though? I claim that for any two numbers, the multiples they share are also multiples of their LCM.

First, I want to come up with a construction for the LCM and then I can prove that all numbers that are multiples of both the numbers of interest must also be a multiple of the LCM. To do this, we first prove the Fundamental Theorem of Arithmetic: for any integer $n > 1$, n is either prime or the product of primes. To prove this, consider some integer m that is neither a prime nor a product of primes. If there is at least one such m, we can gather all such m into a set M and choose m to be the smallest such m. Since m is not a prime it can be written as a product of two integers $m = ab$, where $1 < a < m$ and $1 < b < m$. Since $a, b < m$ they cannot be in the set M. Therefore a and b must be either primes or the product of primes, but then ab is the product of primes, a contradiction. Therefore no such m exists. From here, we can construct the LCM. Consider, c to be the LCM of to integers a and b, and thus $c = q_a a$ and $c = q_b b$, and:

$$\begin{aligned} a &= p_{1a}^{n_{1a}} p_{2a}^{n_{2a}} ... p_{ia}^{n_{ia}} \\ b &= p_{1b}^{n_{1b}} p_{2b}^{n_{2b}} ... p_{jb}^{n_{jb}} \\ c &= p_{1c}^{n_{1c}} p_{2c}^{n_{2c}} ... p_{kc}^{n_{kc}} \end{aligned}$$

are the prime factorizations of a, b, and c. If c is the LCM of a and b, it must contain all of the unique primes on each list. For example, the LCM of $15 = 3(5)$ and $21 = 3(7)$ is $3(5)(7) = 105$ (note, $105 = 7(15)$ and $105 = 5(21)$). Or more generally, the p_{ic} are unique primes from a and b with powers equal to the maximum of the n_{ia} and n_{ib}. To see that a and b are divisors of c as the $n_{ic} \geq n_{ia}$ and $n_{ic} \geq n_{ib}$ for each prime. Thus, we can arrange the primes to produce q_a and q_b, they are both all the primes in the other number not in the original number. As an example, consider $a = 56 = 2^3 7^1$ and $b = 60 = 2^2 3^1 5^1$. In this case, the LCM is $c = 2^3 3^1 5^1 7^1 = 840$, and $q_a = 3^1 5^1 = 15$ and $q_b = 2^1 7^1 = 14$. Note, also, if any of these primes is taken from c, then c is no longer divisible by either a or b, depending on which prime is removed. Thus, because the n_{ic} are as small as possible, we expect c to be a minimum. As a consequence of this construction too, we see that any other multiple, in order to be divisible by a and b must minimally include these prime factors. Thus, it must also be divisible by the least common multiple and the LCM is indeed the smallest as all multiples must have the form:

$$m = q \prod_{i=1}^{n} p_{ic}^{n_{ic}}$$

where $q \geq 1$. This statement relies on the fact that if an integer n is divisible by an integer m it must also be divisible by each of the p_{ib} to their maximum power (as well as lowest power) and all of their products and vice versa, i.e.:

$$n = qm = q \prod_{i=1}^{k} p_{im}^{j_{im}} = q_1 p_{1m}^{j_{1m}} = ... = q_k p_{km}^{j_{km}}$$

This is a lot to say, that prime factorization works the way that we think it should.