Prime Factorization

Chirag Samantaroy

February 19, 2021

1 Definitions

- We say that a divides b, denoted as $a \mid b$, if $b = ac$ for some integer c.
- The prime factorization of a number n is the representation of n as a product of not necessarily distinct primes, written as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where p_i is the ith prime and e_i is the power of p_i in n.

Problem 1.1 (Fundamental Theorem of Arithmetic). Every integer has a unique prime factorization up to the ordering of the prime powers.

2 GCD/LCM

The **greatest common divisor** of two or more integers, which are not all zero, is the largest positive integer that divides each of the integers.

Two integers are **relatively prime** if there is no integer greater than one that divides them both (i.e. $\gcd(m, n) = 1 \iff m, n$ are relatively prime).

Suppose m, n are relative prime integers. By the definition of relatively prime, no prime number can divide both m, n, so if the prime factorizations are

$$\prod_{i=1}^{\infty} p_i^{m_i} \text{ and } \prod_{i=1}^{\infty} p_i^{n_i}$$

respectively, then one of m_i, n_i is 0 for each i. Actually, it turns out that this is sufficient, since

$$\gcd(m, n) = \prod_{i=1}^{\infty} p_i^{\min(m_i, n_i)} = \prod_{i=1}^{\infty} p_i^{0} = 1.$$

The **least common multiple** of two or more integers, which are not all zero, is the smallest positive integer that is a multiple of each of the integers.

Going back, again suppose the prime factorizations of two integers m and n

$$\prod_{i=1}^{\infty} p_i^{m_i} \text{ and } \prod_{i=1}^{\infty} p_i^{n_i}$$

respectively. Then,

$$\operatorname{lcm}(m,n) = \prod_{i=1}^{\infty} p_i^{\max(m_i,n_i)}.$$

Also, it's well-known the formula:

$$\operatorname{lcm}(m,n) = \frac{|mn|}{\gcd(m,n)}.$$

3 Number and Sum of Divisors

Problem 3.1 (Number of Divisors). The **number of divisors** of $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ is

$$\tau(n) = \prod_{i=1}^{k} e_i + 1.$$

Any divisor of $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ is of the form $p_1^{a_1}p_2^{a_2}\cdots p_k^{e_k}$ for some $a_1 \in \{0,1,\ldots,e_1-1,e_1\}, a_2 \in \{0,1,\ldots,e_2-1,e_2\}$, and so on and so forth till $a_k \in \{0,1,\ldots,e_k-1,e_k\}$. (Why?) Hence, there are e_1+1 choices for a_1, e_2+1 choices for a_2, and so on and so forth, for a total of

$$(e_1+1)(e_2+1)\cdots(e_k+1) = \prod_{i=1}^{k} e_i + 1$$

divisors.

Problem 3.2 (Sum of Divisors). The **sum of divisors** of $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ is

$$\sigma(n) = \prod_{j=1}^{k}\sum_{i=0}^{e_j} p^i.$$

4 Examples

Example 4.1 (PuMAC 2007/Number Theory B1). If you multiply all positive integer factors of 24, you get 24^x. Find x.

The prime factorization of 24 is $2^3 \cdot 3$, so there are a total of $(3+1)(1+1) = 4 \cdot 2 = 8$ positive integer factors, and therefore four pairs of factors that multiply to 24. So, our answer is $24^4 \implies \boxed{4}$.

Example 4.2 (PuMAC 2011/Number Theory A1/B3). The only prime factors of an integer n are 2 and 3. If the sum of the divisors of n (including itself) is 1815, find n.

Let $n = 2^a3^b$. We have

$$(1+2+\cdots+2^a)\left(1+3+\cdots+3^b\right) = 1815.$$

By the finite geometric series formula,

$$\begin{aligned}
\left(\frac{1-2^{a+1}}{1-2}\right)\left(\frac{1-3^{b+1}}{1-3}\right) &= 1815 \\
\implies \left(\frac{1-2^{a+1}}{-1}\right)\left(\frac{1-3^{b+1}}{-2}\right) &= 1815 \\
\implies \frac{(1-2^{a+1})(1-3^{b+1})}{2} &= 1815 \\
\implies \left(1-2^{a+1}\right)\left(1-3^{b+1}\right) &= 3630 \\
\implies (2^{a+1}-1)(3^{b+1}-1) &= 3630.
\end{aligned}$$

Notice that $3630 = 15 \cdot 242 = (2^4 - 1)(3^5 - 1)$. So,

$$\begin{aligned}
a + 1 = 4 &\implies a = 3 \\
b + 1 = 5 &\implies b = 4.
\end{aligned}$$

And therefore, our answer is $n = 2^3 3^4 = \boxed{648}$.

Example 4.3 (AMC 10B 2013/9)**.** Three positive integers are each greater than 1, have a product of 27000, and are pairwise relatively prime. What is their sum?

The prime factorization of 27000 is $2^3 \cdot 3^3 \cdot 5^3$. Since $2^3 = 8, 3^3 = 27, 5^3 = 125$ are each greater than 1, have a product of 2700, and are pairwise relatively prime, we say these are the aforementioned three positive integers in the problem statement. Thus, their sum gives an answer of $8 + 27 + 125 = \boxed{160}$.

Example 4.4 (AMC 10B 2013/24)**.** A positive integer n is *nice* if there is a positive integer m with exactly four positive divisors (including 1 and m) such that the sum of the four divisors is equal to n. How many numbers in the set $\{2010, 2011, 2012, \ldots, 2019\}$ are nice?

For an integer n to have four positive divisors, it must either be a perfect cube or a product of two primes. None of the numbers in the set $\{2010, 2011, 2012, \ldots, 2019\}$ are perfect cubes (why?), so we can ignore that case.

If $n = pq$ for two primes p and q, then the sum of the divisors of n is

$$(1 + p)(1 + q),$$

which is equal to n (assuming n is nice).

Case 1: Either p or q are 2. Without loss of generality, assume $p = 2$. Then, $p + 1 = 3 \mid n$, and $q + 1$ remains even. Thus, the only numbers that work are even multiples of 3 which are 2010 and 2016. However, to check these are nice, we need to check if $\frac{2010}{3} - 1$ and $\frac{2016}{3} - 1$ are prime, which they are not. So, we see that in this case none of them work.

Case 2: Both p and q are odd primes. This means that, $p + 1$ and $q + 1$ are both even, resulting in $4 \mid n$. Thus, the only numbers that work are multiples of 4 which are 2012 and 2016. Notice that, $2012 = 4 \cdot 503$, and $503 - 1$ is not a prime. This leaves 2016, which we can show works.

Thus, there is only $\boxed{1}$ number in the set $\{2010, 2011, 2012, \ldots, 2019\}$ that is nice.

Example 4.5 (AMC 10B 2016/12). Two different numbers are selected at random from $\{1, 2, 3, 4, 5\}$ and multiplied together. What is the probability that the product is even?

We complementary count. The only possible way to obtain a product that is odd is if the two numbers selected are both odd. The probability of this happening is $\frac{\binom{3}{2}}{\binom{5}{2}} = \frac{3}{10}$. Thus, the probability that the product is even is $1 - \frac{3}{10} = \frac{7}{10}$.

Example 4.6 (AIME II 2019/3). Find the number of 7-tuples of positive integers (a, b, c, d, e, f, g) that satisfy the following systems of equations:

$$\begin{aligned} abc &= 70, \\ cde &= 71, \\ efg &= 72. \end{aligned}$$

From the system of equations, we deduce

$$\begin{aligned} c \mid 70 \text{ and } c \mid 71 &\implies c \mid \gcd(70, 71) = 1. \\ e \mid 71 \text{ and } e \mid 72 &\implies e \mid \gcd(71, 72) = 1. \end{aligned}$$

Thus, $c = e = 1$. Substituting this into the system of equations

$$\begin{aligned} ab &= 70, \\ d &= 71, \\ fg &= 72. \end{aligned}$$

There are 8 factors of $70 = 2 \cdot 5 \cdot 7$, giving 4 pairs of (a, b), and 12 factors of $72 = 2^3 \cdot 3^2$, giving 6 pairs of (f, g). However, remember a and b can be interchanged, so this gives $4 \cdot 2 = 8$ choices for (a, b) and $6 \cdot 2 = 12$ choices for (f, g). This gives us an answer of $\boxed{96}$.

Example 4.7 (AIME I 2020/4). Let S be the set of positive integers N with the property that the last four digits of N are 2020, and when the last four digits are removed, the result is a divisor of N. For example, $42,020$ is in S because 4 is a divisor of $42,020$. Find the sum of all the digits of all the numbers in S. For example, the number $42,020$ contributes $4 + 2 + 0 + 2 + 0 = 8$ to this total.

There is a positive integer m such that $N = 10^4 m + 2020$. N has the property that $m \mid N$, and since $m \mid 10^4 m$, we need $m \mid 2020$.

Exercise 4.8. Finish the problem off from here!

Example 4.9 (AoPS Wiki). Find the largest integer k for which 2^k divides 27!

For a problem such as this, we need to refer to Legendre's Formula:

Problem 4.10 (Legendre's Formula). **Legendre's Formula** states that

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor,$$

where p is a prime and $v_p(n!)$ is the exponent of p in the prime factorization of $n!$.

Using Legendre's Formula, substituting $n = 27$ and $p = 2$ gives

$$\begin{aligned} v_2(27!) = & \left\lfloor \frac{27}{2} \right\rfloor + \left\lfloor \frac{27}{2^2} \right\rfloor + \left\lfloor \frac{27}{2^3} \right\rfloor + \left\lfloor \frac{27}{2^4} \right\rfloor \\ =& 13 + 6 + 3 + 1 \\ =& 23 \end{aligned}$$

which means that the largest integer k for which 2^k divides $27!$ is $\boxed{23}$.