Unique Factoring: Consequences

Unique prime decomposition (unique factoring) is an important property, so in this section we discuss some its consequences.

Multiplicity

First, let us note that we can group identical factors in the decomposition. In this we get a product of the form

$m = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$.

Here all p_i are different, and all n_i are positive integers (the number of occurrences of p_i in the factorization).

The number n_i is called the *multiplicity* of a prime p_i in m. If p_i does not appear in the decomposition, we say that the multiplicity of p_i in m equals zero. (This sounds natural since we may add fictional term $p_i^0 = 1$ in the factoring.)

Stop and think! Did you notice that the definition of multiplicity relies on the unique factoring theorem? Why?

The multiplicity of p in m is defined by counting the occurrences of p in the prime decomposition of m. Here it is important that we may (due to the unique factorization) speak about *the* prime decomposition of m. In an imaginary world where factorization is not unique, it could happen that, say, prime factor 3 appears 5 times in one factorization of m and appears 7 times in another factorization of the same m. What would then be the multiplicity of 3 in m? Should it be 5 or 7? (Fortunately, we do not have such a problem in the real world.)

Problem

How can we compute the multiplicity of p in ab knowing the multiplicity of p in a and b?

Problem

What is the multiplicity of 2 and 5 in the number $100! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 100$? It is easy to see that the decimal representation of $100!$ ends with several zeros (for example, the factor 100 alone produces 2 zeros). Find out exactly how many trailing zeros appear in $100!$

Divisors and Multiplicity

Problem

Complete the statement: "an integer $d > 1$ is a divisor of an integer $m > 1$ if and only if the multiplicity of p $\langle \ldots \rangle$ for every prime p.

The last part can be filled as follows: "if the multiplicity of p in d does not exceed the multiplicity of p in m, for every prime p". Indeed, imagine that d is a divisor of m, i.e., that $m = dq$ for some q. Then the (unique) factorization of m is obtained by concatenating the factorizations of d and q. Therefore, the multiplicity of every prime p in m is the sum of its multiplicities in d and q, and is greater or equal than the multiplicity of p in d.

On the other hand, if every prime appears in the factorization of m at least as many times as for d, then we can add missing factors to d to obtain m. If q is the product of these missing factors, then $dq = m$, so d divides m.

Problem

Consider all the positive divisors of $2^4 3^3 = 432$. How many of them do exist (including "trivial divisiors" 1 and 432)?

As the previous problem shows, all the divisors have the form $2^k 3^l$ where $0 \le k \le 4$ and $0 \le l \le 3$. For $k = l = 0$ we get 1, for $k = 4$ and $l = 3$ we get 432. We may list all of them systematically:

$2^0 \cdot 3^0 = 1,$

$2^0 \cdot 3^1 = 3,$

$2^0 \cdot 3^2 = 27,$

$2^0 \cdot 3^3 = 81,$

$2^1 \cdot 3^0 = 2,$

$2^1 \cdot 3^1 = 6,$

$2^1 \cdot 3^2 = 54,$

$2^1 \cdot 3^3 = 162, \ \ldots$

We do not need to write them all explicitly; we have only to count them. Each of five powers of 2 (i.e., $2^0, 2^1, 2^2, 2^3, 2^4$) is combined with four powers of 3 (i.e., $3^0, 3^1, 3^2, 3^3$), so we get $5 \times 4 = 20$ combinations that lead (as we know) to 20 divisors.

Problem

How many positive divisors has $2^{10} \cdot 3^{15} \cdot 5^{20}$?

Problem

Find a number that has exactly $1024 = 2^{10}$ divisors.

Here the answer is not unique: one could take a product of any 10 different prime numbers. Then each divisor is determined by 10 bits (whether each of these prime factors is there or not), so we have 2^{10} combinations.

One can also note that 2^k has exactly $k + 1$ divisors, so we may consider 2^{1023} has exactly 1024 divisors.

Problem

What is the minimal positive number that has exactly 15 divisors?

GCD and LCM Revisited

Knowing the prime factorizations of two integers, it is easy to find all their common divisors.

Problem

List all positive common divisors of $2^2 \cdot 3^2 \cdot 5^2$ and $3^3 \cdot 5 \cdot 7^3$.

Common divisors of a and b should have only factors that appear both in a and b, and the multiplicity of such a factor should not exceed its multiplicity both in a and b. In our case common divisor may contain only factors 3 and 5, with multiplicity at most $\min(2, 3) = 2$ and $\min(2, 1) = 1$ respectively. So we can have $3^0 = 1, 3^1 = 3$ or $3^2 = 9$ multiplied either by $5^0 = 1$ or $5^1 = 5$. In total, we have six common divisors $1, 3, 9, 5, 15, 45$. (To get negative divisors, we should put minus sign before the elements of this list.)

The maximal common divisor is therefore $3^2 \cdot 5^1 = 45$. It is easy to see that it is divisible by all other common divisors. The same reasoning can be applied to any other pair a, b.

Problem

Provide another proof of this fact (the greatest common divisor is a multiple of every common divisor) using Euclid's algorithm and diophantine equations.

Hint: if $\gcd(a, b) = d$, then the equation $ax + by = d$ has integer solution (x, y). Now, if d' is some common divisor of a and b, it divides also ax and by.

Problem

Formulate a general recipe: how could one find the greatest common divisor $\gcd(a, b)$ knowing the factorizations of a and b?

The reasoning is as in the example above: only common factors appear in the greatest common divisor of a, b, and the multiplicity of a factor is the minimum of its multiplicity in a and b. One could write this as follows

$\gcd(p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}, p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}) = p_1^{\min(n_1, m_1)} \cdot \ldots \cdot p_k^{\min(n_k, m_k)}$.

This formula assumes that the two numbers contain the same prime factors. If not, one should add missing ones with multiplicity 0 (i.e., factors like p^0). In this way the same formula works for $a = 1$ or $b = 1$ (all multiplicities are zeros, and the greatest common divisor is also 1).

Problem

Write a similar formula for the least common multiple of two numbers in terms of their factorization.

The reasoning could be similar: the common multiples of a and b should include all the factors that appear in a *or* in b, with the same or bigger multiplicities. This shows that

$\mathrm{lcm}(p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}, p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}) = p_1^{\max(n_1, m_1)} \cdot \ldots \cdot p_k^{\max(n_k, m_k)}$.

Problem

Explain why the least common multiple of two numbers $a, b > 1$ divides all other common multiples.

Problem

Using the formulas for $\gcd(\mathrm{a}, \mathrm{b})$ and $\mathrm{lcm}(\mathrm{a}, \mathrm{b})$, give a new proof that

$\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab.$

Hint: $\min(u, v) + \max(u, v) = u + v$.

Problem

Prove the following formula that includes greatest common divisor and least common multiple of three numbers (understood in a natural way):

$\mathrm{lcm}(a, b, c) = \frac{a \cdot b \cdot c \cdot \gcd(\mathrm{a,b,c})}{\gcd(a,b) \cdot \gcd(a,c) \cdot \gcd(b,c).}$

All these formulas may create an impression that one should compute greatest common divisors and least common multiples in two steps: first we find the factorization and then apply our formulas. **This is a very bad idea**: it reduces a relatively easy problem (e.g., finding the greatest common divisor; it can be done rather fast by Euclid's algorithm) to a practically intractable problem of prime factorization!

One special case of the results above is important enough to be stated separately:

Problem

Assume that a is divisible by b and by c, and that b and c are relatively prime ($\gcd(b, c) = 1$). Prove that a is divisible by bc.

This can be explained in different ways. First, we have seen that $bc = \gcd(b, c) \cdot \mathrm{lcm}(b, c)$, so $\mathrm{lcm}(bc) = bc$, and a, being a common multiple of b and c, should be divisible by the least common multiple bc.

Second explanation: since b and c are relatively prime, their factorizations have no common factors. Therefore, the factorization of a (that includes the factorization of b and also the factorization of c) includes the factorization of bc, so $bc | a$.

Finally, one may use diophantine equations: since b and c are relatively prime, then $1 = bx + cy$ for some integers x and y. Multiplying both sides by a, we see that $a = abx + acy$. Here $abx = (a/c)bcx$ is divisible by bc, as well as $acy = (a/b)bcy$, so their sum a is also divisible by bc.

Completed **Go to next item**

Like **Dislike** **Report an issue**