Factoring: Uniqueness

Decomposition of an integer $m > 1$ into a product of prime factors is essentially unique. The word "essentially" here means that we ignore the ordering of the factors: they can be permuted in any way and we still get the same decomposition. For example,

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$$

are all the same decompositions.

Here is a more formal statement:

Theorem

Let $m = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$ be two decompositions of an integer $m > 1$ into products of primes. Then $k = l$ and the lists $[p_1, \ldots, p_k]$ and $[q_1, \ldots, q_l]$ contain the same numbers (can be obtained from each other by a permutation of elements).

Stop and think! Look at the following two factorizations of the same number:

$$78227 \cdot 244999 = 19165536773 = 99599 \cdot 192427$$

Isn't it a counterexample to the unique factoring theorem?

Indeed, we have two essentially different decompositions. But nobody said that the factors are prime. Indeed, we may factor them (e.g., using the programs shown above) and find that

$$78227 = 137 \cdot 571,$$

$$244999 = 337 \cdot 727,$$

$$99599 = 137 \cdot 727,$$

$$192427 = 337 \cdot 571.$$

So both decompositions are obtained from

$$19165536773 = 137 \cdot 337 \cdot 571 \cdot 727$$

by different ways of grouping the factors.

Problem

Find one more decomposition of the same number 19165536773 into a product of five-digit and six-digit factors.

So we do not have a counterexample to the theorem, but how can we prove it? It is not so simple and will use our previous knowledge (in particular, Euclid's algorithm and its consequences).

The argument starts in a natural way. Let us assume that the statement is not true and there are two different decompositions of the same number:

$$p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l,$$

where the lists $[p_1, \ldots, p_k]$ and $[q_1, \ldots, q_l]$ are essentially different (differ more than by a permutation). We need to get a contradiction (that shows that such a counterexample to our statement does not exist).

Let us first look at the lists $[p_1, \ldots, p_k]$ and $[q_1, \ldots, q_l]$. They are different, but still it is possible that they are not disjoint and some prime number appears in both lists. Then we can cancel this factor in both lists and get a smaller counterexample. If there is another common factor in both lists, we cancel it and get a smaller counterexample, and so on. Either we cancel all the factors (but this means that the initial decompositions were essentially the same), or some factors remain (in both sides --- otherwise one side becomes 1 while the other is greater than 1).

In this way, we arrive at a counterexample with disjoint lists, and we have to get a contradiction showing that this cannot happen. As mathematicians put it, *we may assume without loss of generality* that two prime decompositions of the same number m have no common factors:

$$m = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l,$$

Why is it impossible? Consider some factor p_1 in the left hand side. Looking on the left hand side, we note that p_1 is a divisor of m. On the other hand, all factors in the right hand side are prime numbers q_i that are different from p_1 (no common factors assumption) and therefore p_1 is not a divisor of any q_i. We get a contradiction: the product of several numbers that are not divisible by p_1 is divisible by p_1. The theorem is proven.

Stop and think! Do you see a gap in this argument?

The last step says "we get a contradiction: the product of several numbers that are not divisible by [some prime] p_1 is divisible by p_1". But we have not really proven that such a situation is impossible. In other words, to finish the proof we need to prove the following lemma.

Lemma

If some integers $q_1, \ldots, q_l$ are not divisible by some prime p, then their product $q_1 \cdot \ldots \cdot q_l$ is also not divisible by p.

Stop and think! We assume here that p is prime. Is this assumption necessary? (Does the lemma hold without this assumption?)

Consider $p = 4$. Then 6 and 10 are not divisible by p, but their product 60 is. (In terms of factorization it is easy to explain: 6 and 10 have only one factor 2 in the decomposition, while 4 is $2 \cdot 2$, so we need both 6 and 10 to get two factors 2.)

Problem

Provide a counterexample for this statement with $p = 6$

How do we prove the Lemma? For $l = 2$, it claims that the product of two numbers not divisible by a prime p is not divisible by p. This statement can be equivalently reformulated in several ways (all versions prohibit the same case when the product is divisible, but the factors are not):

- if a and b are not divisible by p, then ab is not divisible by p;
- if ab is divisible by p, then either a or b (or both) are divisible by p;
- if ab is divisible by p, and a is *not* divisible by p, then b is divisible by p.

Now you may recall the Euclid's lemma (that was one of the consequences of Euclid's extended algorithm):

Euclid's lemma

If $n|ab$ and $\gcd(a, n) = 1$, then $n|b$.

Our statement is a direct consequence of Euclid's lemma. Indeed, if n is prime and a is not divisible by n, then $\gcd(a, n) = 1$, because n has only two divisors 1 and n, and the latter is not a divisor of a (and therefore not a common divisor).

It remains to prove the same statement for more numbers.

Stop and think! Assume that p is prime and three integers a, b, c are not divisible by p. Can you see why abc is not divisible by p?

We have just shown that $u = ab$ is not divisible by p. Applying the same statement again, now to u and c, we conclude that $uc = abc$ is not divisible by p.

For more numbers: if a, b, c, d are not divisible by p, then ab is not divisible by p, then $abc = (ab) \cdot c$ is not divisible by p, and finally $abcd = (abc) \cdot d$ is not divisible by p. Similar reasoning works for any number of factors, and this finishes the proof of the unique decomposition.

We see that if the product of several number is divisible by p then one of the numbers is divisible by p. This is similar to a well known algebraic rule: if the product of several numbers equals 0 then at least one of the factors equals zero. This algebraic rule can be explained as follows: if, say $ab = 0$ and $a \neq 0$, then we may multiply the first equation by $1/a$ and get $(1/a) \cdot a \cdot b = (1/a) \cdot 0$. Here the left hand side is b (since $a \cdot (1/a) = 1$) and the right hand side is 0, so we get $b = 0$. The same reasoning may be repeated for numbers modulo p: recall that any number $a \not\equiv 0 \pmod{p}$ has an inverse modulo p.

Completed **Go to next item**

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