Dr. Z.'s Number Theory Lecture 6 Handout: The Fundamental Theorem of Arithmetic

By Doron Zeilberger

The prime numbers are the **atoms** of multiplication.

Fundamental Theorem of Arithmetic

Every positive integer n can be written **uniquely** as a product of primes or prime-powers, i.e. for some $k \geq 1$

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \quad ,$$

where $a_1, \dots, a_k$ are positive integers, and $p_1 < p_2 < \dots < p_k$ are primes.

How to do it?

Input: A positive integer n.

Output: A list of pairs $L(n) = [p_1, a_1], [p_2, a_2], \dots, [a_k, b_k]$ ($k \geq 0$, p_i, primes, a_i positive integers, and $p_1 < p_2 < \dots < p_k$, such that

$$n = p_1^{a_1} \cdots p_k^{a_k} \quad .$$

If $n = 1$ then output the **empty list**: NOTHING.

Let p be the smallest prime divisible by n. Let a be the largest integer such that n/p^a is an integer (i.e. that p^a is divisible by n). Then

$$L(n) = [p, a], L(n/p^a)$$

Problem 6.1: Find the prime-power decomposition of 495.

Solution of 6.1: 2 is not divisible by 495, but 3 is. 3^2 is divisible by 495 but 3^3 is not, so $p = 3, a = 2$. So

$$L(495) = [3, 2], L(495/3^2) = [3, 2], L(55) \quad .$$

The smallest prime that divieds 55 is 5. 55 is not divisible by 5^2, so, since $55/5 = 11$

$$L(55) = [5, 1], L(11) \quad .$$

11 is not divisible by 7, but is divisible by 11 (in fact it *is*) 11. 11 is nod divisible by 11^2 so $p = 7, a = 1$, since $11/11^1 = 1$

$$L(11) = [11, 1], L(1)$$

Now it is time for the **backwards** journey. Of course $L(1)$ is the empty list, so

$$L(11) = [11, 1] \quad ,$$

$$L(55) = [5,1], L(11) = [5,1],[11,1] \quad ,$$

$$L(495) = [3,2], L(55) = [3,2],[5,1],[11,1] \quad .$$

Ans. to 6.1: $L(495) = [3,2],[5,1],[11,1]$, or in, humanese

$$495 = 3^2 \cdot 5 \cdot 11 \quad .$$

The **existence** follows immediately from the **algorithm**, but so does **uniqueness** (in spite of what Euclid or wikipedia would tell you). The **smallest** prime divisible by n, and the **largest power** of p divisible by n are both well-defined and *unique*, so both *existence* and *uniqueness* follow by induction.

Multiplying integers given in "product of prime-powers format"

Simply multiply them, simplify the powers, and rearrange in order of increasing primes.

Problem 6.2: Find the product-of-primes-representation of $105 \cdot 2002$, by first doing it for 105 and 2002 (rather than for 210210.

Solution of 6.2:

$$105 = 3 \cdot 5 \cdot 7$$

$$2002 = 2 \cdot 7 \cdot 11 \cdot 13$$

So

$$105 \cdot 1001 = (3 \cdot 5 \cdot 7) \cdot (2 \cdot 7 \cdot 11 \cdot 13) = 2 \cdot 3 \cdot 7^2 \cdot 11 \cdot 13 \quad .$$

Ans. to 6.2: The product-of-prime-powers representation of $105 \cdot 2002$ is $2 \cdot 3 \cdot 7^2 \cdot 11 \cdot 13$, or in list notation

$$[2,1],[3,1],[7,2],[11,1],[13,1] \quad .$$