

# THE JOY OF NUMBERS

## 1. THE FUNDAMENTAL THEOREM OF ARITHMETIC

Today was a very long lecture. We tried to prove the fundamental theorem of Arithmetic and this was not easy at all.

(1.1) **Theorem (The fundamental Theorem of Arithmetic).** *Every integer greater than or equal to two has a unique factorization into prime integers. By the word unique we mean the following: If  $n = p_1 \cdot p_2 \cdots p_s$  and  $n = q_1 \cdot q_2 \cdots q_t$  are two prime factorizations of the integer  $n$  (with the  $p_i$ 's and the  $q_i$ 's written in ascending order) then  $s = t$  (that is, the number of prime factors is the same) and  $p_1 = q_1, p_2 = q_2, \dots, p_s = q_s$ .*

*Proof.* We first decided that we need to prove that every positive integer can be written as product of primes. Eric, suggested the following proof. Assume by contradiction that there exists an integer that cannot be written as product of prime. Let  $S$  be the set of all integers that cannot be written as product of primes. We are assuming that  $S$  is not empty. The set  $S$  is obviously bounded below, because we are looking just at positive integers. But more than that, it is bounded below by 3, because 2 and 3 are primes and therefore they can be written as product of primes. By the axiom of *well ordering* of the integers,  $S$  has a minimal element, call it  $x$ . We noticed that  $x$  is not prime, because if it were prime then it would be a product of prime, and it could not be an element of the set  $S$ . If  $x$  is not prime, then it has factors different from  $x$  itself and 1. Write  $x = ab$ , it follows that  $1 < a < x$  and  $1 < b < x$ . Because  $x$  is the minimal element of the set  $S$ , we can deduce that  $a$  and  $b$  are not in  $S$  and therefore they can be written as product of primes:  $a = p_1 \cdots p_n$  and  $b = q_1 \cdots q_l$ , and therefore  $ab = p_1 \cdots p_n q_1 \cdots q_l$ . This shows that  $x$  can be written as product of primes, contradicting the assumption on  $x$  being an element of  $S$ .

We have already proved that every integer has a prime factorization. We just need to prove the uniqueness business. To do this properly, we will prove it by induction on the number  $s$  of prime factors in the first factorization. (For the purposes of this proof, we will assume  $s \leq t$ . If not, just interchange the two factorizations so that the shorter one comes first.) We first do the case  $s = 1$ . In this case,  $n = p_1$ , so  $n$  is prime. Since  $p_1$  has no other factors other than 1, it is clear that  $q_1 = p_1$ . And  $t = 1$  as well (that is, the second factorization has only one prime factor too). Now assume that the theorem is true whenever the first factorization has  $k$  prime factors. We now prove it for  $k + 1$  factors: Let  $n = p_1 \cdots p_{k+1}$  and  $n = q_1 \cdots q_t$ . Clearly  $p_{k+1}$  (being a prime in the first factorization) divides  $n$ . Therefore,  $p_{k+1}$  divides  $q_1 \cdots q_t$ . Since  $p_{k+1}$  is prime, we know by the proposition below that  $p_{k+1}$  divides  $q_i$  for some  $i$ . Therefore,  $p_{k+1} \leq q_i \leq q_t$ . On the other hand,  $q_t$  divides  $n$ , so  $q_t$  divides  $p_j$  for some  $j$ . Hence,  $q_t \leq p_j \leq p_{k+1}$ . As

$p_{k+1} \leq q_t$  and  $q_t \leq p_{k+1}$  we have  $p_{k+1} = q_t$ . Now cancel  $p_{k+1}$  and  $q_t$  from the equation  $p_1 \cdots p_{k+1} = q_1 \cdots q_t$ , which gives us

$$p_1 \cdots p_k = q_1 \cdots q_{t-1}.$$

But the first factorization now has only  $k$  prime factors. By our induction assumption, we know that the uniqueness property holds for this factorization. Thus, the number of primes appearing in the factorizations must be equal; i.e.,  $k = t - 1$ . This then gives us  $k + 1 = t$ , which is what we wanted. Also by induction, we know we can that  $p_1 = q_1, p_2 = q_2, \dots, p_k = q_k$ . This completes the proof!  $\square$

In the proof we used the following proposition, which proof we decide postpone for a while. In the meantime we will think about the proof as homework.

(1.2) **Proposition.** *Suppose  $p$  is prime and  $a_1, \dots, a_n$  are any  $n$  integers such that  $p$  divides the product  $a_1 \cdot a_2 \cdots a_n$ . Then  $p$  divides  $a_i$  for some  $i$  between 1 and  $n$ .*