

4 Unique factorization

We proved the *fundamental theorem of arithmetic* in the following form.

Theorem 4.1. *Every positive integer n can be written uniquely in the form*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \quad (1)$$

for some $k \geq 0$ where the p_i are distinct prime numbers in increasing order $p_1 < p_2 < \cdots < p_k$ and each $e_i > 0$. The numbers k, p_1, \dots, p_k and e_1, \dots, e_k are uniquely determined by n .

For the homework:

Lemma 4.2. *The number n is a square if and only if every exponent e_i in the prime decomposition (1) is even.*

Proof. This is obvious. If $n = m^2$ then, because of the fact that m has a prime decomposition

$$m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \quad (2)$$

we get

$$n = m^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}.$$

Therefore, every square has even exponents in its prime decomposition.

Conversely, if n has even exponents:

$$n = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}$$

Then $n = m^2$ where m is given by (2). This proves the lemma. □

[This shows that even obvious things take a long time to prove.]

Homework: p.61 #1.62, 63.