Fundamental Theorem of Arithmetic. If $a$ is an integer larger than 1, then $a$ can be written as a product of primes. Furthermore, this factorization is unique except for the order of the factors.

PROOF: There are two things to be proved. Both parts of the proof will use the Well-ordering Principle for the set of natural numbers.

(1) We first prove that every $a > 1$ can be written as a product of prime factors. (This includes the possibility of there being only one factor in case $a$ is prime.) Suppose bwoc that there exists a integer $a > 1$ such that $a$ cannot be written as a product of primes. By the Well-ordering Principle, there is a smallest such $a$. Then by assumption $a$ is not prime so $a = bc$ where $1 < b, c < a$. So $b$ and $c$ can be written as products of prime factors (since $a$ is the smallest positive integer than cannot be.) But since $a = bc$, this makes $a$ a product of prime factors, a CONTRADICTION.

(2) Now suppose bwoc that there exists an integer $a > 1$ that has two different prime factorizations, say $a = p_1 \cdots p_s = q_1 \cdots q_t$, where the $p_i$ and $q_j$ are all primes. (We allow repetitions among the $p_i$ and $q_j$. That way, we don’t have to use exponents.) Then $p_1 | a = q_1 \cdots q_t$. Since $p_1$ is prime, by the Lemma above, $p_1 | q_j$ for some $j$. Since $q_j$ is prime and $p_1 > 1$, this means that $p_1 = q_j$. For convenience, we may renumber the $q_j$ so that $p_1 = q_1$. We can now cancel $p_1$ from both sides of the equation above to get $p_2 \cdots p_s = q_2 \cdots q_t$. But $p_2 \cdots p_s < a$ and by assumption $a$ is the smallest positive integer with a non–unique prime factorization. It follows that $s = t$ and that $p_2, \ldots, p_s$ are the same as $q_2, \ldots, q_t$, except possibly in a different order. But since $p_1 = q_1$ as well, this is a CONTRADICTION to the assumption that these were two different factorizations. Thus there cannot exist such an integer $a$ with two different factorizations. √