One of the most fundamental theorems in number theory is the famous Euclid's division lemma:

Theorem 1. *Let $q \in \mathbb{N}$. Each natural number n has a unique representation of the form*

$$n = m \cdot q + r$$

with $m, r \geq 0$ and $r < q$.

Proof. For the cases $q = 1, n = 1$ resp. $q > 1, n = 1$ the unique solutions with $m = 1$, $r = 0$ resp. $m = 0$, $r = 1$ are implied.
We first proof the existence of the representation by induction over n. So let us assume for some $r < q$ we have

$$n = m \cdot q + r$$

Then $n + 1$ can be written as

$$n + 1 = m \cdot q + r$$

If $r + 1 < q$ we are done. If $r + 1 = q$, we can write

$$n + 1 = (m + 1) \cdot q$$

For proving uniqueness, assume

$$n = m_1 \cdot q + r_1 = m_2 \cdot q + r_2$$

Without loss of generality assume $m_2 > m_1$. Then

$$(m_2 - m_1) \cdot q + r_2 - r_1 = 0$$

This yields,

$$q \leq (m_2 - m_1) \cdot q = r_1 - r_2$$

which results in the contradiction $r_1 \geq q$. We conclude, $m_1 = m_2$. From

$$m_1 \cdot q + r_1 = m_1 \cdot q + r_2$$

we finally see $r_1 = r_2$. $\square$

Lemma 2. *Let $a, b, p \in \mathbb{N}$ with p being a prime number. The product $a \cdot b$ is divisible by p if and only if either a or b is divisible by p.*

Proof. If either a or b is divisible by p it is clear that then its product is divisible by p as well.
In case $a = b = 1$ the statement is trivially true. We proceed by induction on the value of each factor, that is, we assume the statement is true for all numbers a', b' with $a' < a$ and $b' < b$.
Assume $a \cdot b$ is divisible by p but none of a or b is. Then for some unique positive r_1, r_2 we have

$$a = m_1 \cdot p + r_1$$

$$b = m_2 \cdot p + r_2$$

with

$$r_1, r_2 < p \tag{1}$$

This yields,

$$a \cdot b = (m_1 m_2 q + r_1 m_2 + m_1 r_2) \cdot p + r_1 \cdot r_2$$

with $r_1 \cdot r_2 > 0$. Moreover, by divisibility assumption, there must be $m \in \mathbb{N}$ with

$$r_1 \cdot r_2 = m \cdot p$$

Since $r_1 < a$ and $r_2 < b$, by inductive assumption either r_1 or r_2 must be divisible by p. But this contradicts (1) and thus we must drop the assumption of neither a nor b not being divisible by p. $\square$

Lemma 3. *Let p be a prime number. A product of natural numbers is divisible by p if and only if at least one of its factors is divisible by p.*

Proof. This can be seen by induction on the length of the product and application of the previous lemma. For instance, $a \cdot b \cdot c = (a \cdot b) \cdot c$. □

The previous lemma can be used to proof the following theorem.

Theorem 4. *Each natural number n greater than 1 has a unique prime decomposition.*

Proof. The statement is trivially fulfilled in case if n is any prime number. So let us suppose n is not a prime number and the statement is fulfilled by induction for all natural numbers below of n. Then there are some $a, b \in \mathbb{N}$ such that $n = a \cdot b$ and $a, b > 1$. Since obviously $a, b < n$, both have a prime decomposition which leads altogether to a prime decomposition of n.

The uniqueness of such a decomposition can be seen as follows:

Assume

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_i^{m_i}$$

and

$$n = q_1^{k_1} \cdot q_2^{k_2} \cdots q_j^{k_j}$$

where $\{p_1, p_2, \ldots, p_i\}$ and $\{q_1, q_2, \ldots, q_j\}$ are sets of primes. Without loss of generality let us assume that $p_1 \notin \{q_1, q_2, \ldots, q_j\}$, then since n is divisible by p_1, the product $q_1^{k_1} \cdot q_2^{k_2} \cdots q_j^{k_j}$ must it be as well. The lemma implies that at least one factor must be divisible by p_1, but this contradicts the q's being prime numbers. Since p_1 has been chosen arbitrarily, this shows

$$\{p_1, p_2, \ldots, p_i\} = \{q_1, q_2, \ldots, q_j\}$$

Therefore we may assume to have two decompositions of the form

$$p_1^{m_1} \cdot p_2^{m_2} \cdots p_i^{m_i} = p_1^{k_1} \cdot p_2^{k_2} \cdots p_i^{k_i}$$

By repeatedly applying the lemma we observe the l.h.s must be divisible k_1 times by p_1 and that the only factor allowing this is $p_1^{m_1}$. This implies $m_1 \geq k_1$. The same argumentation we can do with the remaining prime numbers and moreover by interchanging the role of the l.h.s and r.h.s. This finally yields $m_1 = k_1, \ldots, m_i = k_i$. $\square$

Theorem 5. *There are infinitely many prime numbers.*

Proof. To the contrary assume the set of primes is finite and given by $P := \{p_1, p_2, \ldots, p_n\}$. Consider the number

$$q := p_1 \cdot p_2 \cdots p_n + 1$$

By theorem 1, q is not divisible by any of the p_i's. Nor can q be a prime number since it would be greater than all of the p_i's. By theorem 4 there must exist some prime number p that divides q. As mentioned $p \notin P$ in contradiction to the assumption. So we conclude, there must exist infinite many primes. $\square$

Theorem 6. *The prime decomposition of a non-prime natural number n with $n > 1$ contains a prime number p with*

$$p \leq \lfloor \sqrt{n} \rfloor$$

Proof. Assume $n = p_1 \cdot p_2 \cdots p_m$ being a prime decomposition with possible repetitions in the prime number $[p_1, \ldots, p_m]$. There cannot be two factors p_i, p_j with

$$p_i, p_j > \lfloor \sqrt{n} \rfloor$$

since otherwise $p_i \cdot p_j > n$. $\square$

Theorem 7. *Each prime number greater than* 3 *is of the form either* $6n - 1$ *or* $6n + 1$.

Proof. Just note, $6n + 2$, $6n + 4$ are divisible by 2 and $6n + 3$ by 3. So, only $6n + 1$ or $6n + 5$ possibly can be prime. $\square$