WELL ORDERING PRINCIPLE.

There is another form of induction that is sometimes useful:

Theorem. *(the well-ordering principle) If A is a non-empty set of natural numbers, then it has a smallest element.*

Note that this is false if you ask for A to be a non-empty set of integers ($\mathbb{Z}$ itself has no smallest element) or of positive rationals ($\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$ has no smallest element).

Proof. Suppose that A has no smallest element; then we have to show that A is empty. We prove the following by induction on n:

$$\text{for all } n \in \mathbb{N},\ 1, 2, \dots, n \text{ are all not in } A.$$

Base case. When $n = 1$, we have to show that 1 is not in A. But if 1 were in A then it would be the smallest element of A, since 1 is the smallest natural number. As A has no smallest element, this is a contradiction.

Induction step. Suppose that $1, 2, \dots, n$ are not in A (the induction hypothesis). We have to show that $1, 2, \dots, n, n+1$ are not in A; the only new thing is to show that $n+1$ is not in A. Suppose for contradiction that $n+1$ *is* in A. Then it is not be the smallest element of A because A has no smallest element. So there must be a natural number $k < n+1$ in A. But then k is one of $1, 2, \dots, n$, all of which are not in A, so we have a contradiction. Therefore $n+1$ is not in A, as required.

So for every n, we have shown that $1, 2, \dots, n$ are not in A; in particular, every n is not in A, so A is empty! □

As an application, we prove:

Proposition. *Every rational number can be written in lowest terms. That is, every $q \in \mathbb{Q}$ can be written as $q = \frac{a}{b}$ where a and b are integers with no common factor greater than one.*

Proof. Let A be the set of values of $|b|$ for all fractions $\frac{a}{b}$ which *cannot* be written in lowest terms. We want to show that all fractions can be written in lowest terms, in other words that A is empty.

Suppose that A is not-empty. Then by the well-ordering principle it has a smallest element, b. Therefore there is a fraction $\frac{a}{b}$ which cannot be written in lowest terms, but so that $\frac{c}{d}$ can be written in lowest terms whenever $|d| < |b|$.

Since $\frac{a}{b}$ is not in lowest terms, there is a common factor $m \geq 2$ of a and b, so $a = mA$ and $b = mB$ for integers A, B. But then $|B| < |b|$, so $\frac{A}{B}$ *can* be written in lowest terms. But $\frac{a}{b} = \frac{A}{B}$, so $\frac{a}{b}$ can be written in lowest terms — contradiction! □

This proof formalises the idea that to write a rational number in lowest terms we just keep dividing out common factors until we can't any more. Proofs that involve a process (like dividing out) and a natural number quantity that keeps getting smaller (like the absolute value of the denominator) can often be written using the well-ordering principle.

Remark. It is in fact true that every rational number can be written *uniquely* in lowest terms with positive denominator. But this is much harder to prove!!!

Exercise. A prime number is a natural number greater than one which has no positive factors except for one and itself. Prove that every natural number can be written as a product of prime numbers. Can you prove that this way of writing it is unique?