**Number theory** is the study of the arithmetical properties of the integers.

You have been working with integers since you were in pre-Kindergarten, but these objects have never been formalized for you before. What *is* an integer?

In 1895, Giuseppe Peano crafted axioms for the integers that succeeded in such a formalization:

The **natural numbers** form a set $\mathbb{N}$ with the following properties.
1. (a) $1 \in \mathbb{N}$ (that is, $\mathbb{N}$ is not the empty set);
2. (b) Every $x \in \mathbb{N}$ has a unique successor $x' \in \mathbb{N}$ (whence we write $2 = 1', 3 = 2', 4 = 3'$, etc.)
3. (c) $1$ is not the successor of any $x \in \mathbb{N}$;
4. (d) [Principle of Induction] If $S$ is a subset of $\mathbb{N}$ so that
   - $1 \in S$, and
   - whenever $x \in S$ then $x' \in S$, 
   then $S = \mathbb{N}$.

These axioms are sufficiently powerful to derive all of arithmetic. For instance,

**Proposition** For all $x \in \mathbb{N}$, $x' \neq x$.

**Proof** Let $S = \{x \in \mathbb{N} \mid x' \neq x\}$. By Axiom (c), $1 \in S$. Also, if $x \in S$, then $x' \neq x$. But if $(x')' = x'$, we would have by Axiom (b) that $x' = x$, a contradiction. So $(x')' \neq x'$, whence $x' \in S$. It follows by Axiom (d) that $S = \mathbb{N}$. //
**Proposition**  For every $x \in \mathbb{N}$ different from 1, there exists a $y \in \mathbb{N}$ for which $x = y'$.

**Proof** Let $S = \{x \in \mathbb{N} \mid x = 1$ or $\exists y$ with $x = y'\}$. Then certainly $1 \in S$. Also, if $x \in S$ is different from 1 then its successor $x'$ must be in $S$ by definition of $S$. By induction therefore, $S = \mathbb{N}$. //

We can formally define **addition** on the natural numbers:
- For every $x \in \mathbb{N}$, let $x+1$ be defined as $x'$; and
- For any $y \in \mathbb{N}$, define $x+y' = (x+y)'$.

**Example**

\[ 5 + 3 = 5 + 2' \]
\[ = (5 + 2)' \]
\[ = (5 + 1)' \]
\[ = ((5 + 1)')' \]
\[ = ((5')')' = (6')' = 7' = 8 \]

The familiar properties of associativity and commutativity of addition now follow from the Peano axioms.

**Theorem** \((x + y) + z = x + (y + z)\)

**Proof** Take first the case $z = 1$:

\[ (x + y) + 1 = (x + y)' = x + y' = x + (y + 1). \]
Now assume inductively that the property holds for some particular larger value of \( z \); then

\[
(x + y) + z' = ((x + y) + z)'
= (x + (y + z))'
= x + (y + z)'
= x + (y + z')
\]

So the property holds for all \( z \). //

**Proposition** \( x + 1 = 1 + x \)

**Proof** Let \( S = \{ x \in \mathbb{N} \mid x + 1 = 1 + x \} \). Clearly, \( 1 \in S \). If now \( x \in S \) then \( x' = x + 1 = 1 + x \), so

\[
x' + 1 = (1 + x) + 1 = 1 + (x + 1) = 1 + x'
\]

whence \( x' \in S \). It follows by Axiom (d) that \( S = \mathbb{N} \). //

**Theorem** \( x + y = y + x \)

**Proof** By the previous proposition we know that the relation holds when \( y = 1 \). So now assume inductively that the property holds for any particular value of \( y \); then

\[
x + y' = x + (y + 1) = (x + y) + 1
= (y + x) + 1 = y + (x + 1)
= y + (1 + x) = (y + 1) + x
= y' + x
\]
We could continue this development to show how Peano’s axioms lead to formal definitions that extend \( \mathbb{N} \) by defining the number 0 and the concept of additive inverse \((-x)\) and the subtraction operation to obtain the larger set \( \mathbb{Z} \) of all integers, positive, negative and zero. (\( \mathbb{Z} \) stands for the Ger. *zahlen* = Eng. *number*.) We could also define formally the ordering relations \(<\) and \(>\) for integers, and the operation of multiplication — along with its familiar properties (notably the distributive law \( x(y + z) = xy + xz \)). But all this would take us too far from our focus.

Instead let us remind ourselves that Peano’s Axiom (d) is often called the **Weak Principle of Induction** to distinguish it from

**[The Strong Principle of Induction]** If \( S \) is a subset of \( \mathbb{N} \) so that
- \( 1 \in S \), and
- whenever all of 1, 2, 3, \( \ldots \), \( x \in S \) then \( x' \in S \),
then \( S = \mathbb{N} \).

This is a stronger form of the principle since it appears to require a more stringent condition for the set \( S \) (*all of 1, 2, 3, \( \ldots \), \( x \in S \)) than is required in the Weak Principle of Induction. However, as we will soon see, both Induction Principles are logically equivalent to each other: the weak form is no weaker than the strong form. Indeed, both principles are also equivalent to a more straightforward property of the natural numbers:
[The Well-Ordering Principle] Every nonempty subset of \( \mathbb{N} \) has a least element.

Theorem The following are logically equivalent:
  
  I. The Weak Principle of Induction
  II. The Strong Principle of Induction
  III. The Well-Ordering Principle

Proof [I \( \Rightarrow \) II.] Suppose that \( T \subseteq \mathbb{N} \) satisfies \( 1 \in T \), and that whenever \( 1, 2, \ldots, x \in T \) it follows that \( x+1 \in T \) as well. We want to use Weak Induction to prove that \( T = \mathbb{N} \). So let \( S = \{ x \in \mathbb{N} \mid \text{all of } 1, 2, \ldots, x \in T \} \).

Certainly \( 1 \in S \). Also, if \( x \in S \), then \( 1, 2, \ldots, x \in T \), so by the definition of \( T \), \( x+1 \in T \). But then all of \( 1, 2, \ldots, x, x+1 \in T \), so \( x+1 \in S \), too. By the Weak Induction Principle applied to \( S \), we conclude that \( S = \mathbb{N} \). As this implies that \( T = \mathbb{N} \), we have deduced that the Strong Principle of Induction holds.

[II \( \Rightarrow \) III.] Let \( U \) be a subset of \( \mathbb{N} \) that has no least element. Then define \( T = \{ x \in \mathbb{N} \mid x \notin U \} \). If \( 1 \in U \), then since \( 1 \) is not the successor of any natural number, it is the least element of \( U \), contradicting the definition of \( U \). So \( 1 \notin U \Rightarrow 1 \in T \). If \( 2 \in U \), then since \( 1 \notin U \), \( 2 \) would be the least element of \( U \), another contradiction. Thus, \( 2 \notin U \Rightarrow 2 \in T \). Continuing in this way, we can show that for any \( x \in \mathbb{N} \), we must have \( 1, 2, \ldots, x \in T \). So by Strong Induction applied to the set \( T \), we conclude that \( T = \mathbb{N} \). But then \( U \) must be empty. So any nonempty subset of \( \mathbb{N} \) must have a least element.
Suppose that \( S \subseteq \mathbb{N} \) satisfies \( 1 \in S \), and that whenever \( x \in S \) it follows that \( x+1 \in S \) as well. Then define \( U = \{ x \in \mathbb{N} | x \notin S \} \). If \( U \) is nonempty, then by the Well-Ordering Principle, it has a least element \( x \). Since \( 1 \in S \), \( x \) cannot be \( 1 \), so \( x \) is the successor of some \( y \in \mathbb{N} \). Since \( x \) is the least element of \( U \), \( y \notin U \Rightarrow y \in S \). But by the definition of \( S \), \( x = y+1 \in S \) as well. But this is impossible, because \( x \in S \Rightarrow x \notin U \), meaning that \( x \) cannot be the least element of \( U \). This contradiction implies that the assumption that \( U \) was nonempty must be false; that is, \( U = \emptyset \). But then \( S = \mathbb{N} \), which shows that the Weak Induction Principle holds. //

We conclude with three examples showing how these principles can be useful tools for proving theorems about the natural numbers.

**Example** of the Weak Induction Principle at work:

**Theorem** Let \( F_1 = 1, F_2 = 1 \), and \( F_{n+1} = F_n + F_{n-1} \) recursively define the (familiar) Fibonacci numbers. Then for all \( n \geq 1 \),

\[
\sum_{k=1}^{n} F_k^2 = F_n F_{n+1}.
\]

**Proof** (Let \( S \) be the set of subscripts \( n \) for which the formula holds; we will show by Weak Induction that \( S = \mathbb{N} \).) The case \( n = 1 \) is clear as \( 1^2 = 1 \cdot 1 \). If we assume that the formula holds for some particular choice of \( n \), then
\[
\sum_{k=1}^{n+1} F_k^2 = \left( \sum_{k=1}^{n} F_k^2 \right) + F_{n+1}^2 \\
= F_n F_{n+1} + F_{n+1}^2 \\
= F_{n+1} (F_n + F_{n+1}) \\
= F_{n+1} F_{n+2}
\]

which shows that the formula holds for subscript \( n+1 \). //

**Example of the Strong Induction Principle at work:**

**Theorem** Every \( n \geq 2 \) is a product of prime numbers.

**Proof** (Let \( T \) be the set of numbers \( x \) for which \( x+1 \) is a product of prime numbers; we will show by Strong Induction that \( T = \mathbb{N} \).) The case \( x = 1 \) is clear, since 2 is a prime number itself. Next, suppose the theorem is true for all \( x \) with \( 1 \leq x \leq n \). If \( n+1 \) is a prime number, then we’re done. (Why?) Otherwise, it factors: \( n+1 = ab \) where \( 2 \leq a, b \leq n \). By our (strong) induction hypothesis, both numbers \( a \) and \( b \) are products of prime numbers, so their product is as well. This completes the proof. //

**Example of the Well-Ordering Principle at work:**

**Theorem** \( \sqrt{2} \) is irrational.

**Proof** If \( \sqrt{2} \) is rational, then the set

\[
U = \{ q \in \mathbb{N} | \sqrt{2} = \frac{p}{q} \text{ for some } p \in \mathbb{N} \}
\]

is nonempty. By the Well-Ordering Principle, it has a
least element, which we label $b$. So there is some $a \in \mathbb{N}$ for which $\sqrt{2} = \frac{a}{b}$. Since $1 < \sqrt{2} < 2$, we can write

$$1 < \frac{a}{b} < 2 \quad \Rightarrow \quad b < a < 2b \quad \Rightarrow \quad 0 < a - b < b .$$

But then

$$2 = \frac{a^2}{b^2} \quad b^2 = \frac{a^2}{2b} \quad 2b^2 - ab = a^2 - ab \quad b(2b - a) = a(a - b) \quad \sqrt{2} = \frac{a}{b} = \frac{2b - a}{a - b}$$

showing that $a - b < b$ is an element of $U$, contradicting the minimality of $b$. It follows that $\sqrt{2}$ cannot be rational. //