Definition of the Integers
MTH230 Fall 2014.
(based off notes of Armstrong)

Definition 1

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

Definition 2

Let $\mathbb{Z}$ be a set equipped with

- an **equivalence relation** "=" defined by
  - (reflexive) $\forall a \in \mathbb{Z}, a = a$
  - (symmetric) $\forall a, b \in \mathbb{Z}, a = b \implies b = a$
  - (transitive) $\forall a, b, c \in \mathbb{Z}, (a = b AND b = c) \implies a = c$
- a **total ordering** "$\leq$" defined by
  - (antisymmetric) $\forall a, b \in \mathbb{Z}, (a \leq b AND b \leq a) \implies a = b$
  - (transitive) $\forall a, b, c \in \mathbb{Z}, (a \leq b AND b \leq c) \implies a \leq c$
  - (total) $\forall a, b \in \mathbb{Z}, a \leq b OR b \leq a$
- and two binary operations (functions from $\mathbb{Z}^2 \to \mathbb{Z}$)
  - (addition) $\forall a, b \in \mathbb{Z}, \exists a + b \in \mathbb{Z}$
  - (multiplication) $\forall a, b \in \mathbb{Z}, \exists ab \in \mathbb{Z}$ (sometimes written $a \cdot b$)

  which satisfy the following properties.

Axioms of Addition

(A1)	$\forall a, b \in \mathbb{Z}, a + b = b + a$	(commutative)
(A2)	$\forall a, b, c \in \mathbb{Z}, a + (b + c) = (a + b) + c$	(associative)
(A3)	$\exists 0 \in \mathbb{Z}, \forall a \in \mathbb{Z}, 0 + a = a$	(additive identity exists)
(A4)	$\forall a \in b, \exists b \in \mathbb{Z}, a + b = 0$	(additive inverses exist)

These four axioms say that $\mathbb{Z}$ with $+$ is an *additive group*. There is a special element called 0 that is an "identity element" for addition. Every integer a has an "additive inverse" which we call $-a$.

Axioms of Multiplication

(M1)	$\forall a, b \in \mathbb{Z}, ab = ba$	(commutative)
(M2)	$\forall a, b, c \in \mathbb{Z}, a(bc) = (ab)c$	(associative)
(M3)	$\exists 1 \in \mathbb{Z}, 1 \neq 0, \forall a \in Z, 1a = a$	(multiplicative identity exists)

Note that elements of $\mathbb{Z}$ do NOT have a "multiplicative inverse". So $\mathbb{Z}$ with multiplication is not a group.

Axiom of Distribution

(D) $\forall a, b, c \in \mathbb{Z}, a(b + c) = ab + ab$

This shows how addition and multiplication interact.

Together, these eight axioms say that $\mathbb{Z}$ with $+$ and $\cdot$ is a *(commutative) ring*.

Now we describe how arithmetic and order interact.

Axioms of Order

(O1) $\forall a, b, c \in \mathbb{Z}, a \leq b \implies a + c \leq b + c$

(O2) $\forall a, b, c \in \mathbb{Z}, (a \leq b AND 0 \leq c) \implies ac \leq bc$

(O3) $0 < 1$ (that is, $0 \leq 1 AND 0 \neq 1$)

These first eleven properties say that $\mathbb{Z}$ is an *ordered ring*.

However we have not yet defined $\mathbb{Z}$. There are other ordered rings; for example the real numbers $\mathbb{R}$.

We need one more subtle axiom to distinguish $\mathbb{Z}$. It is not obvious...

First, let $\mathbb{N} = \{a \in \mathbb{Z} \colon 1 \leq a\}$ denote the set of **natural numbers**.

The Well-Ordering Axiom

(WO) $\forall X \subset \mathbb{N}, X \neq \emptyset, \exists a \in X, \forall b \in X, a \leq b$

That is, "Every non-empty subset of $\mathbb{N}$ has a smallest element."

This is also known as the **principle of induction**.

Definition 3

Condensed, most efficient definition of $\mathbb{Z}$ due to Giuseppe Peano (1858-1932).

Peano's Axioms

Let $\mathbb{N}$ be a set equipped with

- an equivalence relation "=" and
- a unary "successor" operator $S \colon \mathbb{N} \to \mathbb{N}$

satisfying:

(P1)	$1 \in \mathbb{N}$	(an element called 1 is in $\mathbb{N}$)
(P2)	$\forall n \in \mathbb{N}, S(n) \neq 1$	(1 is not the successor of any natural number)
(P3)	$\forall m, n \in \mathbb{N}, S(m) = S(n) \implies m = n$	(S is an injective function)
(P4)	If a set $K \subset \mathbb{N}$ satisfies $1 \in K$ and $\forall n \in \mathbb{N}, n \in K \implies S(n) \in K$, then $K = \mathbb{N}$	(The induction principle)

Then with lots of work, one can use $\mathbb{N}$ and S to define $\mathbb{Z}$ with all the axioms from Definition 2.