Let $n$ be a natural number. Let us define the following relation on $\mathbb{Z}$:

$$a \equiv b \pmod{n} \text{ if } n \text{ divides } b - a$$

**Theorem 1** $\equiv$ is an equivalence relation.

**Definition 2** The equivalence classes of integers under this relation are called residue classes modulo $n$. We denote it by $\mathbb{Z}_n$.

**Theorem 3** There are exactly $n$ residue classes modulo $n$.

When we want to name one of the classes, we just take an element of it. For convenience, many times we label the classes with the elements $0, 1, \ldots, n - 1$.

Just like with the Cauchy completion, the operators on $\mathbb{Z}$ naturally extend to $\mathbb{Z}_n$.

**Definition 4** For $a, b \in \mathbb{Z}_n$ let $x \in a$, $y \in b$ and let

$$a + b = \overline{x + y}$$
$$a \cdot b = \overline{x \cdot y}$$

where $\overline{z}$ denotes the residue class of $z \in \mathbb{Z}$.

**Theorem 5** $+$ and $\cdot$ are well-defined on $\mathbb{Z}_n$. $(\mathbb{Z}_n, +, \cdot)$ is a ring.

This means that modulo $n$ one can do the same kind of algebraic manipulations as you are used to in $\mathbb{Z}$.

**Exercise 6** Solve the following congruences:

1) $2x + 1 \equiv 3 \pmod{5}$;
2) $x^2 \equiv 1 \pmod{17}$;
3) $2x \equiv 5 \pmod{8}$;
4) $3x \equiv 3 \pmod{6}$;

As you see in 3) and 4), there is something to be careful about. Namely, the simplification rule does not always work. For example, 3 does not have a multiplicative inverse modulo 6 so $3x \equiv 3 \pmod{6}$ does not imply $x \equiv 1 \pmod{6}$. But if you think about it, 3 does not have a multiplicative inverse in $\mathbb{Z}$ as well. Let us put this into a bit more abstract setting.
Definition 7 Let $R$ be a ring. An element $0 \neq a \in R$ is a zero divisor if there exists $0 \neq b \in R$ with $ab = 0$.

You can easily check that $\mathbb{Z}$ does not have nontrivial zero divisors.

Exercise 8 What are the zero divisors modulo 6, 7 and 12?

This is the real notion what we need for simplification.

Lemma 9 Let $0 \neq a \in R$ be a non-zero-divisor. Then $ax = ay$ implies $x = y$.

In fact, for finite rings non-zero-divisors are exactly the invertible elements.

Theorem 10 Let $R$ be a finite ring. Then $0 \neq a \in R$ has a multiplicative inverse if and only if $a$ is not a zero divisor.

This theorem has various consequences.

Definition 11 For a prime $p$ let $\mathbb{F}_p = \mathbb{Z}_p$.

Theorem 12 For a prime $p$ every nonzero element of $\mathbb{F}_p$ is invertible.

In other terms, $\mathbb{F}_p$ is a field. A quick corollary:

Theorem 13 (Wilson’s theorem) Let $p$ be a prime. Then

$$(p - 1)! \equiv -1 \pmod{p}$$

Some basics modulo $p$.

Theorem 14 For all $a, b \in \mathbb{F}_p$ we have

$$(a + b)^p = a^p + b^p.$$ 

Theorem 15 (Fermat’s Little theorem) Let $p$ be a prime and let $a$ be an integer. Then

$$a^p \equiv a \pmod{p}.$$ 

Corollary 16 Let $p$ be a prime and let $a$ be an integer not divisible by $p$. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$ 

Let us understand what this really means.

Theorem 17 Let $R$ be a finite ring and let $a \in R$ be invertible. Then there exists a natural $k$ with $a^k = 1$.

Definition 18 The minimal $n$ with the above property is called the multiplicative order of $a$. We denote it by $o(a)$.

Theorem 19 Let $0 \neq a \in \mathbb{F}_p$. Then $o(a)$ divides $p - 1$. 

2
Let us get back to modulo $n$.

**Theorem 20** Let $a$ be an integer and let $n$ be a natural number. Then the following are equivalent:
1) $a$ is relatively prime to $n$;
2) $a$ is invertible modulo $n$;
3) there exist integers $x, y$ with $ax + ny = 1$.

**Definition 21** (Euler’s totient function) For a natural number $n$ let $\mathbb{U}(n)$ denote the set of invertible elements in $\mathbb{Z}_n$. Let $\phi(n)$ be the size of $\mathbb{U}(n)$.

**Exercise 22** Find a formula for $\phi(n)$.

**Lemma 23** If $a, b \in \mathbb{U}(n)$ then $ab \in \mathbb{U}(n)$.

**Theorem 24** Let $0 \neq a \in \mathbb{Z}_n$ be invertible. Then $o(a)$ divides $\phi(n) - 1$.

Hint: look at a certain graph on $\mathbb{U}(n)$.

**Theorem 25** (Euler’s theorem) Let $n$ be a natural number and let $a$ be an integer relatively prime to $n$. Then
\[ a^{\phi(n)} \equiv a \pmod{n} \]

Of course, you don’t really need integers to play the modulo game. For example, you can take $\mathbb{R}[x]$ and a nonzero polynomial $p(x) \in \mathbb{R}[x]$ and for $q(x), r(x)$ define
\[ q(x) \equiv r(x) \pmod{p(x)} \text{ if } p(x) \text{ divides } r(x) - q(x) \]

The same way you can define the residue classes and $\mathbb{R}[x]$ modulo $p(x)$ becomes a ring. In fact, that is the easiest way to define complex numbers.

**Definition 26** Complex numbers are $\mathbb{R}[x]$ modulo $x^2 + 1$.

We will also give a more down to earth definition later and show that it is the same.