Lecture we defined ring and field (commutative ring where we can divide elements) and saw that \( \mathbb{Z}_n \) is a field \( \iff \) \( p \) is prime.

Let us see another example of a ring.

Ex. Let \( \mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \} \) where multiplication and addition is defined as it is for the complex numbers. Verify that \( \mathbb{Z}[i] \) is a ring and find out which elements in \( \mathbb{Z}[i] \) have a multiplicative inverse. Is \( \mathbb{Z}[i] \) a field?

\( \mathbb{Z}[i] \) is a ring: \( \mathbb{Z}[i] \) inherits the axioms from \( \mathbb{C} \). We only need to check that \( 0 \in \mathbb{C} \) is in \( \mathbb{Z}[i] \) (it obviously is) and that if \( a + bi \in \mathbb{Z}[i] \) then also it's additive inverse \( -a - bi \in \mathbb{Z}[i] \) and this is also evident. Commutativity is also inherited from \( \mathbb{C} \).

In \( \mathbb{C} \) we can form a multiplicative inverse of \( a + bi \) (unless \( a = b = 0 \)) by

\[
\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i
\]

This inverse is in \( \mathbb{Z}[i] \) \( \iff \) \( \frac{a}{a^2 + b^2} \) and \( \frac{b}{a^2 + b^2} \) are...
both integers. \( \Rightarrow \) \( a^2 + b^2 \mid a \) and \( a^2 + b^2 \mid b \) and \( a + bi \neq 0 \). 

Case I: \( a = 0 \) then \( a^2 + b^2 \mid a \Rightarrow b^2 \mid b \Rightarrow b = -1, 0, 1 \). 
This results in \( a + ib = -i, 0, i \) not allowed.

Case II: \( a \neq 0 \) then \( a^2 + b^2 \mid a \Rightarrow a^2 + b^2 \leq |a| \Rightarrow b = 0 \) and \( a = -1, 1, i, -i \) resulting in \( a + ib = -1, 1 \).

The only invertible elements in \( \mathbb{Z}[i] \) are \( \pm 1 \) and \( \pm i \). Thus \( \mathbb{Z}[i] \) is not a field.

**Isomorphisms between rings**

Given two rings \( R, S \) and a bijective map \( f: R \rightarrow S \) such that

\[
\begin{align*}
    f(a +_R b) &= f(a) +_S f(b) \\
    f(a \circ_R b) &= f(a) \circ_S f(b)
\end{align*}
\]

for all \( a, b \in R \), \( f \) is called an isomorphism and \( R, S \) isomorphic rings.

\( \mathbb{E} \quad M = \{(a - b) | a, b \in \mathbb{R} \} \) with ordinary matrix addition and multiplication.

\( M \) is a ring (check \( A, B \in M \Rightarrow A \cdot B \in M \)) \( A + B \in M \).
Now define $f$ by $f : M \to \mathbb{C}$
\[
f\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right) = a + ib
\]

- It is clear that $f$ is surjective since any given $a + ib \in \mathbb{C}$ we get this element as the image of $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M$.

- Also $f$ is injective because if $f(A) = 0$
  then $a = b = 0 \implies A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ the zero of $M$

This shows that $f$ is bijective.

Now check that $f$ preserves the ring operations.

Let $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, $C = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$.

\[
\begin{aligned}
f(A + C) &= f\left(\begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix}\right) = (a+c) + i(b+d)
\end{aligned}
\]

\[
\begin{aligned}
f(A) + f(C) &= f\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right) + f\left(\begin{pmatrix} c & -d \\ d & c \end{pmatrix}\right) = (a + ib) + (c + id) = a + c + i(b + d)
\end{aligned}
\]

OK $f(A + C) = f(A) + f(C)$

\[
\begin{aligned}
f(AC) &= f\left(\begin{pmatrix} (a & b)(c & -d) \\ b & a \end{pmatrix}\right) = f\left(\begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{pmatrix}\right)
\end{aligned}
\]

\[
\begin{aligned}
&= (ac-bd) + i(bc+ad)
\end{aligned}
\]

\[
\begin{aligned}
f(A) f(C) &= (a+ib)(c+id) = (ac-bd) + i(ad+bc)
\end{aligned}
\]

We have now seen that $f(AC) = f(A)f(C)$.

We conclude from all the above that $\mathbb{N}$ and $\mathbb{C}$ are isomorphic.
Last lecture we saw that in \( \mathbb{Z}_n \) an \( a \) is invertible \( \iff (a,n) = 1 \). It follows that

**Thm:** \( \mathbb{Z}_n \) is a field \( \iff n \) is a prime

**Proof:** All non-zero elements \([1],[2],\ldots,[n-1]\) are invertible \( \iff 9, 12, \ldots, n-1 \) are all relatively prime to \( n \) \( \iff n \) is a prime.

---

**Finite fields and RSA-cryptography**

**Thm:** If \( F \) is a finite field with \( q \) elements \( a \in F \) and \( a \neq 0 \) then \( a^{q-1} = 1 \) in \( F \)

**Proof:** Look at \( F^* = \{ x \in F \mid x \neq 0 \} = \{ x_1, x_2, \ldots, x_{q-1} \} \)

\( g: F^* \rightarrow F^* \) given by \( x_i \mapsto ax_i \) is bijective (verify this). Hence \( ax_1, ax_2, \ldots, ax_{q-1} \) is just the list \( x_1, x_2, \ldots, x_{q-1} \) in a different order.

Therefore \( (ax_1)(ax_2)\cdots(ax_{q-1}) = x_1x_2\cdots x_{q-1} \)

\[
\Rightarrow a^{q-1} x_1x_2\cdots x_{q-1} = x_1x_2\cdots x_{q-1} \quad \text{Y is invertible}
\]

\[
\Rightarrow a^{q-1} = 1 \quad \text{The proof is complete!}
\]
In the special case where \( F = \mathbb{Z}_p \) (\( p \) prime), we get \( a^{p-1} \equiv 1 \mod p \) for any \( a \) not divisible by \( p \). This is called Fermat's little theorem.

& Compute \( 19^{34} \mod 11 \)

By Fermat \( 19^{10} \equiv 1 \mod 11 \). Now

\[
19^{34} = 19^{3 \cdot 10 + 4} = (19^{10})^3 \cdot 19^4 \equiv 1^3 \cdot 19^4 \equiv 8^4 \equiv (64)^2 \\
\equiv (-2)^2 \equiv 4
\]

Ans \( 19^{34} \equiv 4 \mod 11 \)

We can generalize Fermat's theorem to products of primes (Fermat \( \Rightarrow a^{m(p-1)+1} \equiv a \) for all int. \( a \) and pos int. \( m \))

Thm 2.4 Let \( p, q \) be different primes and \( m \) a positive integer. Then

\[
a^{m(p-1)(q-1)+1} \equiv a \mod pq
\]

Proof: If we show that \( p \mid \frac{a^{m(p-1)(q-1)+1} - a}{b} \) and \( q \mid \frac{a^{m(p-1)(q-1)+1} - a}{b} \) we also know that \( pq \mid b \) and then we are done.
Computing modulo $p$ we have for $p | a$

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

by Fermat and hence

$$a^{m(p-1)(q-1)+1} = (a^{p-1})^{mq-1} \cdot a \equiv 1^{mq-1} \cdot a = a$$

so $p | a$ if $p | a$. If $p | a$

we also have that $p | a^m(p-1)(q-1)+1 - a$

Exactly the same argument shows that $q | b$

and thus completes the proof by the

comment on the previous page

Ex RSA-system i Cryptography

(Rivest, Shamir and Adelman 1978)

If for ex the bank want many customers to send secret information they can use the following idea:

Start out with two large primes $p, q$

let $n = p \cdot q$. Choose some $d$ with

$$(d, (p-1)(q-1)) = 1$$

and compute the inverse $e$ of $d$ in $\mathbb{Z}_{(p-1)(q-1)}$.

Now $n$ and $e$ are made public but $d$ is secret.
To encode a number $C$ ($1 \leq C \leq n$) compute $D = C^e \mod n$ and send $D$ to the bank. The bank knows $d$ and can then compute $D^d = (C^e)^d = C^{ed} = C^{1 + k(p-1)(q-1)} \equiv C \mod n$.

The message is decoded!

If you can find the factors $p$ and $q$ of $n$ you know $(p-1)(q-1)$ and can compute $d$ and hence break the code. But factorisation is very computationally demanding so with large enough $p,q$ the bank should be safe.

Chinese remainder theorem

Solving systems of congruences like

$$\begin{cases} x \equiv 3 \pmod{5} \quad (1) \\ x \equiv 1 \pmod{7} \quad (2) \\ x \equiv 2 \pmod{11} \quad (3) \end{cases}$$

A pair of congruences can be turned into a diophantine equation. For ex

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{7} \end{cases} \iff \exists a, b \in \mathbb{Z} \text{ such that } x = 3 + 5a = 1 + 7b. \text{ We can find all } a, b \text{ with } 3 + 5a = 1 + 7b \iff 7b - 5a = 2 \quad (*)$$
Solve \((x)\): \((5, 7) = 1\) - Perform the Euclidean algorithm

\[
\begin{align*}
7 &= 5 + 2 \\
5 &= 2 \cdot 2 + 1
\end{align*}
\]

back subst.

\[
\begin{align*}
1 &= 5 - 2 \cdot 2 \\
&= 5 - 2(7 - 5) \\
&= 5 \cdot 3 - 2 \cdot 7
\end{align*}
\]

\[
\left(1 = 5 \cdot 3 - 2 \cdot 7\right) \text{ gives a solution } \begin{cases} b = -24 \\ a = -6 \end{cases}
\]

\[2 = 5 \cdot 6 - 4 \cdot 7\]

all solutions are given by \[
\begin{align*}
a &= -6 + 7k \\
b &= -4 + 5k \quad k \in \mathbb{Z}
\end{align*}
\]

For \(x\) this results in \(x = 3 + 5a =\)

\[
3 + 5(-6 + 7k) = -27 + 35k \quad \text{(or } x = 1 + 7b = \quad 1 + 7(-4 + 5k) = -27 + 35k )
\]

The solution is \(x \equiv -27 \pmod{35} \equiv 8 \pmod{35}\)

But the above method only deals with two congruences. For three or more congruences we must repeat the process above or use

Thm 2.7 (The Chinese remainder theorem)

Assume that the integers \(n_1, n_2, \ldots, n_k\) are pairwise relatively prime. Then the system
\[
\begin{align*}
\begin{cases}
  x \equiv a_1 \pmod{n_1} \\
  x \equiv a_2 \pmod{n_2} \\
  \vdots \\
  x \equiv a_k \pmod{n_k}
\end{cases}
\end{align*}
\]

has a unique solution modulo 
\[n = n_1 n_2 n_3 \cdots n_k\]

Proof: First we find a solution \(x\).

Let \(N_i = \frac{n}{n_i}\). Then \((N_i, n_i) = 1\) so we can find (using the Euclidean algorithm) \(s_i\) and \(t_i\) with 
\[1 = s_i N_i + t_i n_i\]

Multiplying by \(a_i\): 
\[a_i = a_i s_i N_i + a_i t_i n_i\]

Then we can see that 
\[a_i s_i N_i \equiv \begin{cases} a_i \pmod{n_i} \\ 0 \pmod{n_j} \quad (j \neq i) \end{cases}\]

Let 
\[x = a_1 s_1 N_1 + a_2 s_2 N_2 + \cdots + a_k s_k N_k\]

Regarding \(x \pmod{n_i}\), we only get 
\[a_i s_i N_i = a_i - a_i t_i n_i \equiv a_i\] so \(x\) is a solution.

It's also easy to see that \(x + k n\) for \(k \in \mathbb{Z}\) are solutions too.

Uniqueness of solution:

Assume \(x\) and \(x'\) are both solutions to the system. Then \(\mod{n_i}: \) 
\[x - x' \equiv a_i - a_i = 0\]
\[ \Rightarrow n_i \mid x - x'. \quad \text{Thus holds for } i=1,2,\ldots, k = n = n_1 n_2 \ldots n_k \mid x - x' \quad \text{in other words } x \equiv x' \mod n \]

In this step we are using the fact that the \( n_i \) are pairwise relatively prime.

The proof also provide a method for finding the solution. Let's try to use it:

**Ex** Solve \( \begin{cases} x \equiv 3 \mod 5 \\ x \equiv 1 \mod 7 \\ x \equiv 2 \mod 11 \end{cases} \)

Here \( n = 5 \cdot 7 \cdot 11 = 385 \) we will find a unique solution modulo 385.

\[
\begin{align*}
n_1 &= 5 \\
N_1 &= \frac{5 \cdot 7 \cdot 11}{5} = 7 \cdot 11 = 77 \\
n_2 &= 7 \\
N_2 &= \frac{5 \cdot 7 \cdot 11}{7} = 5 \cdot 11 = 55 \\
n_3 &= 11 \\
N_3 &= \frac{5 \cdot 7 \cdot 11}{11} = 5 \cdot 7 = 35
\end{align*}
\]

Compute \( a_i s_i N_i \) :

\[
(5, 77) = 7 \\
77 = 11 \cdot 7 + 0
\]

\[
\begin{align*}
1 &= 5 - 2 \cdot 2 \\
1 &= 5 - 2(77 - 11 \cdot 5) \\
&= 31 \cdot 5 - 2 \cdot 77
\end{align*}
\]

\[
\frac{t_1 n_1}{s_i N_i} = \frac{5 - 2 \cdot 2}{2 \cdot 77} = \frac{31 \cdot 5 - 2 \cdot 77}{2 \cdot 77} = \frac{-462}{77}
\]

\[
a_i s_i N_i = 3 \cdot (-2) \cdot 77 = -462
\]
\[ a_2 S_2 N_2: \quad (7, 55) = 1 \quad 55 = 7 \cdot 8 - 1 \implies \]
\[
1 = \frac{7 \cdot 8 - 55}{t_2 a_2 - S_2 N_2}
\]

\[ a_2 S_2 N_2 = 1 \cdot (-1)(55) = -55 \]

---

Compute \( a_3 S_3 N_3 \): (11, 35) = 1

\[
\begin{align*}
1 & = 11 - 5 \cdot 2 = 11 - 5(35 - 3 \cdot 11) = 16 - 11 - 5 \cdot \frac{35}{t_3 n_3 - S_3 N_3} \\
& = 11 = 5.2 + 1
\end{align*}
\]

\[ a_3 S_3 N_3 = 2(-5)(35) = -350 \]

\[ x = a_1 S_1 N_1 + a_2 S_2 N_2 + a_3 S_3 N_3 = -462 - 55 - 350 = -77 - 55 + 35 = -97 \]

\[ (\text{Check mod 5:} \quad -97 \equiv 3) \]
\[ (\text{mod 7:} \quad -97 \equiv -20 \equiv 1 \quad \text{OK!}) \]
\[ (\text{mod 11:} \quad -97 \equiv 2) \]

Aas: The solutions of the system are those \( x \in \mathbb{Z} \) satisfying\( x \equiv -97 \mod 385 \).