Now we will introduce a mathematical structure that is central to cryptography. This structure uses modular arithmetic.

**Definition:** Let \( m \) be an integer with \( m > 1 \). We define the ring \( \mathbb{Z}_m \) with operations \( \oplus \) and \( \otimes \) as follows.

\[ \mathbb{Z}_m = \{ 0, 1, 2, \ldots, m-1 \} \]

If \( a, b \in \mathbb{Z}_m \), then

\[ a \oplus b = a + b \pmod{m} \]
\[ a \otimes b = a \cdot b \pmod{m} \]

**Example:** Let's examine \( \mathbb{Z}_4 \).

\[ \mathbb{Z}_4 = \{ 0, 1, 2, 3 \} \]

Addition in \( \mathbb{Z}_4 \): \( a \oplus b = a + b \pmod{4} \)

So, for example, \( 2 \oplus 3 = 2 + 3 \pmod{4} = 5 \pmod{4} = 1 \)

Multiplication in \( \mathbb{Z}_4 \): \( a \otimes b = a \cdot b \pmod{4} \)

So, for example, \( 2 \otimes 3 = 2 \cdot 3 \pmod{4} = 6 \pmod{4} = 2 \)

Here are some more examples:

\( 0 \oplus 1 = 1 \), \( 1 \oplus 2 = 0 \), \( 2 \oplus 1 = 3 \), \( 3 \oplus 2 = 0 \)
\( 0 \otimes 1 = 0 \), \( 1 \otimes 3 = 3 \), \( 2 \otimes 1 = 2 \), \( 3 \otimes 3 = 1 \), \( 2 \otimes 2 = 0 \)
We can write two tables which show us how to compute in \( \mathbb{Z}_4 \). First, the addition table.

\[
\begin{array}{cccc}
+ & 0 & 1 & 2 & 3 \\
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\]

Notice that \( a + 0 = 0 + a = a \). 0 is called the additive identity.

Notice that each element \( a \) has an additive inverse, denoted \(-a\), such that \( a + (-a) = 0\).

\[
\begin{align*}
0 + 0 &= 0  \\
1 + 3 &= 0  \\
2 + 2 &= 0  \\
3 + 1 &= 0 \\
\end{align*}
\]

0 is the additive inverse of \( 0 \).

3 is the additive inverse of \( 1 \).

2 is the additive inverse of \( 2 \).

1 is the additive inverse of \( 3 \).

Now, the multiplication table for \( \mathbb{Z}_4 \).

\[
\begin{array}{cccc}
\times & 0 & 1 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 0 & 2 \\
3 & 0 & 3 & 2 & 1 \\
\end{array}
\]

Notice that \( a \times 1 = a \). 1 is called the multiplicative identity.
The multiplicative inverse of a, denoted \( a^{-1} \) ("a inverse") if it exists, has the property that \( a \cdot a^{-1} = 1 \).

We see that 1 has itself as a multiplicative inverse since \( 1 \cdot 1 = 1 \). 3 has itself as a multiplicative inverse since \( 3 \cdot 3 = 1 \). 0 and 2 have no multiplicative inverses.

The ring \( \mathbb{Z}_n \) has several important properties which we will not discuss at this time. However, we do care about multiplicative inverses. When does an element of \( \mathbb{Z}_n \) have one? If the element has a multiplicative inverse, what is it? To investigate this matter we first give a formal definition of multiplicative inverses.

**Definition:** If \( a \in \mathbb{Z}_n \) and there is an element \( a^{-1} \) in \( \mathbb{Z}_n \) such that \( a \cdot a^{-1} = 1 \), then \( a^{-1} \) is called the multiplicative inverse of \( a \).

In \( \mathbb{Z}_4 \), we saw that only 1 and 3 have multiplicative inverses. \( 1^{-1} = 1 \) and \( 3^{-1} = 3 \).

**Definition:** If \( a \) and \( b \) are integers, then the largest integer that divides both \( a \) and \( b \) (or is a factor of \( a \) and \( b \)) is called the greatest common divisor of \( a \) and \( b \) and is denoted \( \text{gcd}(a, b) \).
Examples: \[ \gcd(12, 16) = 4 \] 4 is the largest integer that divides both 12 and 16.

\[ \gcd(36, 48) = 12 \]
\[ \gcd(27, 25) = 1 \]

Here is a theorem which will help us determine when an element of \( \mathbb{Z}_m \) has a multiplicative inverse.

**Theorem:** If \( a \in \mathbb{Z}_m \), then \( a \) has a multiplicative inverse if and only if \( \gcd(a, m) = 1 \).

To illustrate what this theorem says, consider \( \mathbb{Z}_4 \). We saw that \( 1 \) and \( 3 \) have multiplicative inverses in \( \mathbb{Z}_4 \), while \( 0 \) and \( 2 \) do not. Notice that \( \gcd(1, 4) = 1 \) and \( \gcd(3, 4) = 1 \), but \( \gcd(0, 4) = 4 \neq 1 \) and \( \gcd(2, 4) = 2 \neq 1 \).

**Example:** Does \( 6 \) have a multiplicative inverse in \( \mathbb{Z}_9 \)?

If so, what is it?

\[ \gcd(6, 9) = 3 \]

6 does not have a multiplicative inverse in \( \mathbb{Z}_9 \) since \( \gcd(6, 9) \neq 1 \).

**Example:** Does \( 2 \) have a multiplicative inverse in \( \mathbb{Z}_9 \)?

If so, what is it?

Since \( \gcd(2, 9) = 1 \), then \( 2^{-1} \) exists. To find \( 2^{-1} \), we could compute \( 2 \cdot 1, 2 \cdot 2, \ldots \) until the result is 1, but we can reduce the amount of work with a small observation.
Suppose \( a^{-1} = b \) in \( \mathbb{Z}_m \), then \( b^{-1} = a \) since \( a \odot b = 1 \). This means that the multiplicative inverse of \( a \) in \( \mathbb{Z}_m \) is another element in \( \mathbb{Z}_m \) that has a multiplicative inverse. In other words, \( \gcd(a^{-1}, m) = 1 \).

In \( \mathbb{Z}_m \), the elements with multiplicative inverses are 1, 2, 4, 5, 7, and 8. Since \( 1^{-1} = 1 \) (\( 1 \odot 1 = 1 \)), then \( a^{-1} \) is either 2, 4, 5, 7 or 8.

\[
\begin{align*}
2 \odot 2 &= 2 \cdot 2 \pmod{9} = 4 \pmod{9} = 4 \quad 2^{-1} \neq 2 \\
2 \odot 4 &= 2 \cdot 4 \pmod{9} = 8 \pmod{9} = 8 \quad 2^{-1} \neq 4 \\
2 \odot 5 &= 2 \cdot 5 \pmod{9} = 10 \pmod{9} = 1 \pmod{9} = 1
\end{align*}
\]

\( 2^{-1} = 5 \)

We did not need to compute \( 2 \odot 7 \) or \( 2 \odot 8 \).

**Example:** Does 7 have a multiplicative inverse in \( \mathbb{Z}_{10} \)? If so, what is it?

Since \( \gcd(7, 10) = 1 \), then 7\(^{-1} \) exists. The possible candidates for 7\(^{-1} \) are 3, 7, and 9 since \( 1^{-1} = 1 \) and 0, 2, 4, 5, 6 and 8 do not have multiplicative inverses.

\[
7 \odot 3 = 7 \cdot 3 \pmod{10} = 21 \pmod{10} = 1 \pmod{10} = 1
\]

\( 7^{-1} = 3 \)
Finite Fields

Definition: Let \( p \) be a positive integer with \( p > 1 \). We say that \( p \) is prime if the only positive integer divisors of \( p \) are 1 and \( p \).

Example: 43 is prime.

44 = 4 \cdot 11 \) so 44 is not prime.

If \( p \) is a prime number, then the ring \( \mathbb{Z}_p \) is a very special mathematical object called a field. You are already very familiar with fields. For example \( \mathbb{Q} \) (the rational numbers), \( \mathbb{R} \) (the real numbers), and \( \mathbb{C} \) (the complex numbers) are all fields. The fields \( \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) are infinite, while \( \mathbb{Z}_p \) is finite (it has \( p \) elements).

Certain types of finite fields are important in cryptography. In this part of the lesson, you will learn how to work with these fields.

Definition: Suppose \( \mathbb{F} \) is a field. A polynomial of degree \( n \) with coefficients in \( \mathbb{F} \) is an expression of the form

\[ a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \]

where \( a_0, a_1, \ldots, a_n \) are elements of \( \mathbb{F} \) and \( x \) is a variable. The collection of all polynomials with coefficients in \( \mathbb{F} \) is denoted \( \mathbb{F}[x] \).
Example: You are very familiar with \( \mathbb{R}[x] \). It is the collection of polynomials in which the coefficients are real numbers. Examples of elements of \( \mathbb{R}[x] \) are \( 4x^2 - 2x + 7 \), \( x^4 + 7x^3 - x^2 + 5x \), and \( x^4 + 1 \). You already know how to add, subtract, multiply, and divide polynomials in \( \mathbb{R}[x] \).

\[
\begin{align*}
( x^3 + 4x^2 - 5x + 1 ) + ( x^2 - 2x - 8 ) & = x^3 + 5x^2 - 7x - 7 \\
( x^3 + 4x^2 - 5x + 1 ) - ( x^2 - 2x - 8 ) & = x^3 + 4x^2 - 5x + 1 - x^2 + 2x + 8 = x^3 + 3x^2 - 3x + 9 \\
( x^3 + 4x^2 - 5x + 1 ) \cdot ( x^2 - 2x - 8 ) & = x^5 - 2x^4 - 9x^3 + 4x^4 - 8x^2 - 32x^3 - 5x^2 + 10x^3 + 40x + x^2 - 2x - 8 \\
& = x^5 + 2x^4 - 21x^3 - 21x^2 + 38x - 8
\end{align*}
\]

\[
x + 6 \in \text{Quotient}
\]

\[
\overbrace{x^2 - 2x - 8} \middle| \overbrace{x^3 + 4x^2 - 5x + 1}^{\text{Divisor}}
\]

\[
\begin{align*}
x^2 - 2x - 8 & \quad 6x^2 + 3x + 1 \\
& \quad 6x^2 - 12x - 48 \\
& \quad 15x + 49 \in \text{Remainder}
\end{align*}
\]

\[
x^3 + 4x^2 - 5x + 1 = (x^2 - 2x - 8)(x + 6) + (15x + 49)
\]

\[
\text{Divisor} \cdot \text{Quotient} + \text{Remainder}
\]

If you have forgotten how to do division of polynomials, you will need to learn it again.

Example: Let \( p \) be a prime number. We want to work with \( \mathbb{Z}_p[x] \). In particular, we want to work with \( \mathbb{Z}_2[x] \).
Recall that $\mathbb{Z}_2 = \{0,1\}$ where $a \oplus b = a + b \pmod{2}$ and 
$a \odot b = a \cdot b \pmod{2}$ where $a$ and $b$ are in $\mathbb{Z}_2$. For convenience, we will now write $a + b$ instead of $a \oplus b$ and $a \cdot b$ instead of $a \odot b$. This means that in $\mathbb{Z}_2$, $0 + 0 = 0$, $0 + 1 = 1$, $1 + 1 = 0$, $0 \cdot 0 = 0$, $0 \cdot 1 = 1$, $1 \cdot 1 = 1$. Arithmetic in $\mathbb{Z}_2$ is very simple.

The coefficients of a polynomial in $\mathbb{Z}_2[x]$ are either 0 or 1.

Two examples are $x^3 + x^2 + x + 1$ and $x^2 + 1$ ($x^4 + 0 \cdot x + 1$).

Additionally, subtraction, multiplication and division in $\mathbb{Z}_2[x]$ are done exactly like they are done in $\mathbb{R}[x]$ except the coefficients are in $\mathbb{Z}_2$ and not $\mathbb{R}$.

\[
x + x = 2x = 0 \quad x = 0 \\
\uparrow 2(\text{mod } 2) = 0(\text{mod } 2)
\]

\[
(x^3 + x^2 + x + 1) + (x^2 + 1) = x^3 + x^2 + x + x + 1 + 1 = x^3 + x \\
\underline{0 + 0} \\

(x^3 + x^2 + x + 1) - (x^2 + 1) = x^3 + x^2 + x + 1 - x^2 - 1 = x^3 + x
\]

\[
(x^3 + x^2 + x + 1) \cdot (x^2 + 1) = x^5 + x^3 + x^2 + x^2 + x + x + 1 \\
= x^5 + x^3 + x + 1 \quad x^3 + x^3 = 0 \\
\]

For a division example, we will compute the following.

\[
\frac{x^3 + x + 1}{x + 1}
\]
\[
\begin{align*}
\frac{x^2 + x}{x+1} &\quad \frac{x^3 + x^2}{x^2 + x + 1} \\
\frac{x^3 + x^2}{x^2 + x + 1} &\quad 0 - 1 = 1 \text{ in } \mathbb{Z}_2 \quad \rightarrow x^2 + x + 1 \\
&\quad x^4 + x \\
&\quad \text{1} \leftarrow \text{What you need to be able to find.}
\end{align*}
\]

\[x^3 + x + 1 = (x+1)(x^2+x) + 1\]

Note: In \(\mathbb{R}[x]\), \((x+1)(x^2+x)+1 = x^3+x^2+x^2+x+1 = x^3+2x^2+x+1\) not \(x^3+x+1\).

When you learned algebra, you spent a lot of time learning how to factor polynomials in \(\mathbb{R}[x]\). For instance,
\(6x^2 + 5x - 21 = (3x+7)(2x-3)\). Some polynomials cannot be factored in \(\mathbb{R}[x]\). For example, \(x^4 + 1\) cannot be factored in \(\mathbb{R}[x]\). We say that \(x^4 + 1\) is irreducible in \(\mathbb{R}[x]\).

It is interesting to note that \(x^4 + 1\) is irreducible in \(\mathbb{R}[x]\), but it is not irreducible in \(\mathbb{Z}_2[x]\) or \(\mathbb{C}[x]\).

\[
\begin{align*}
\mathbb{R}[x]: &\quad x^4 + 1 \text{ irreducible} \\
\mathbb{C}[x]: &\quad x^4 + 1 = (x-i)(x+i) \quad (i^2 = -1) \\
\mathbb{Z}_2[x]: &\quad x^4 + 1 = (x+1)(x+1) \\
&\quad (x+1)(x+1) = x^4 + x^2 + x + 1 = x^2 + 1 \text{ in } \mathbb{Z}_2[x]
\end{align*}
\]

We will use polynomials that are irreducible in \(\mathbb{Z}_2[x]\) (such as \(x^2+x+1\)) to make special fields that are used in cryptography. The irreducible polynomial you need will be given to you each time.
you will not need to find it.

We will now define a field called $GF(2^n)$ where $n$ is an integer larger than one. The letters $GF$ stand for Galois Field ("gal who field") in honor of the great mathematician Évariste Galois (1811-1832) who first developed the theory of finite fields. You need to know three things about $GF(2^n)$: (1) the elements in $GF(2^n)$, (2) how to add two elements in $GF(2^n)$, and (3) how to multiply two elements in $GF(2^n)$.

(1) The elements of $GF(2^n)$ are the polynomials of $\mathbb{Z}_2[x]$ which have degree less than $n$.

$$GF(2^2) = \{ 0, 1, x, x+1 \} \quad GF(2^2) \text{ has } 4 = 2^2 \text{ elements}$$

$$GF(2^3) = \{ 0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1 \} \quad 8 = 2^3 \text{ elements}$$

$$GF(2^4) = \{ 0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1 \} \quad 16 = 2^4 \text{ elements}$$

(2) Addition of two polynomials in $GF(2^n)$ is the same as addition in $\mathbb{Z}_2[x]$.

In $GF(2^4)$: \[ (x^3 + x+1) + (x^3 + x^2 + 1) = x^3 + x+1 + x^3 + x^2 + 1 = x^2 + x \] \[ x^3 + x^3 = 0 \] \[ 1 + 1 = 0 \]
(3) Multiplication in $\mathbb{GF}(2^n)$ is a two-step process. If $p(x)$ and $q(x)$ are in $\mathbb{GF}(2^n)$ then we compute $p(x) \cdot q(x)$ as follows.

A) Compute $p(x), q(x)$ in $\mathbb{Z}_2[x]$.

B) Find the remainder $r(x)$ when $p(x) \cdot q(x)$ is divided by $\kappa(x)$ where $\kappa(x)$ is an irreducible polynomial of degree $n$ in $\mathbb{Z}_2[x]$.

$$p(x) \cdot q(x) = r(x)$$

Example: Compute $(x^2+1)(x^4+x+1)$ in $\mathbb{GF}(2^3)$. Use the irreducible polynomial $\overline{x^3+x+1}$. Irreducible in $\mathbb{Z}_2[x]$.

A) In $\mathbb{Z}_2[x]$: $(x^2+1)(x^4+x+1) = x^6 + x^3 + x^2 + x + 1$
\[= x^4 + x^3 + x + 1\]

B) In $\mathbb{Z}_2[x]$: $x^3 + x + 1 \vert x^4 + x^3 + 0 \cdot x^2 + x + 1$
\[x^4 + x^3 + x\]
\[x^2 + x + 1\]
\[x^3 + x + 1\]
\[x^2 + x \leftrightarrow \text{In } \mathbb{GF}(2^3)\]

Conclusion: $(x^2+1)(x^4+x+1) = x^2 + x$
Problems

1) Write the addition and multiplication tables for $\mathbb{Z}_6$.

2) Write the addition and multiplication tables for $\mathbb{Z}_7$.

3) Does 20 have a multiplicative inverse in $\mathbb{Z}_{25}$? If so, find it.

4) Does 4 have a multiplicative inverse in $\mathbb{Z}_{13}$? If so, find it.

5) Which elements in $\mathbb{Z}_{21}$ have multiplicative inverses? Find the multiplicative inverse of each of these elements.

6) Which elements in $\mathbb{Z}_{24}$ have multiplicative inverses? Find the multiplicative inverse of each of these elements.

7) Compute each of the following in $\mathbb{Z}_2[x]$.
   A) \((x^4 + x^3 + 1) + (x^2 + x + 1)\)
   B) \((x^4 + x^3 + x + 1) - (x^4 + x^3 + x^2 + 1)\)
   C) \((x+1)(x^2 + x)\)
   D) \((x^4 + x^3 + x^2 + 1)(x^4 + x^3 + x)\)

8) Find the remainder from each of the following divisions in $\mathbb{Z}_2[x]$.
   A) \(\frac{x^4 + x^2 + x + 1}{x^3 + 1}\)
   B) \(\frac{x^5 + x^3 + x^2 + x}{x + 1}\)
   C) \(\frac{x^6 + x + 1}{x^2 + 1}\)
9) Do the following in $GF(2^3)$. For multiplication, use the irreducible polynomial $x^3 + x + 1$.

A) $(x^4 + x) + (x^2 + x + 1)$  
B) $x^3 + (x^2 + 1)$  
C) $x \cdot (x+1)$  
D) $x^4 (x^2 + x)$  
E) $(x^2 + 1)(x^4 + 1)$  
F) $(x^2 + x + 1)(x^3 + x)$

10) List the elements of $GF(2^5)$ as a set.

11) Do the following in $GF(2^5)$. For multiplication, use the irreducible polynomial $x^5 + x^2 + 1$.

A) $(x^4 + x^3 + x) + (x^2 + x + 1)$  
B) $x \cdot x^4$  
C) $(x+1)(x^4 + x + 1)$  
D) $x^4(x^4 + x^2 + x)$  
E) $(x^4 + x^3 + x^2 + 1)(x^4 + x^2 + 1)$
Copyright ©2019 Scott P. Randby

This work is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) or later version license.

License summary: https://creativecommons.org/licenses/by/4.0/

License legal code: https://creativecommons.org/licenses/by/4.0/legalcode