Mathematical Foundations of Cryptography

• Cryptography is based on mathematics
  – In this chapter we study finite fields, the basis of the Advanced Encryption Standard (AES) and elliptical curve cryptography
  – In chapter 8 we study modular arithmetic in more detail as the basis of RSA encryption

• The topics we cover now are
  – Groups, rings, and fields
  – Modular arithmetic and polynomial arithmetic
  – Finite fields of the form GF(p) where p is prime and GF(2^n)
KEY POINTS

- Modular arithmetic is a kind of integer arithmetic that reduces all numbers to one of a fixed set \([0, \ldots, n - 1]\) for some number \(n\). Any integer outside this range is reduced to one in this range by taking the remainder after division by \(n\).
- The greatest common divisor of two integers is the largest positive integer that exactly divides both integers.
- A field is a set of elements on which two arithmetic operations (addition and multiplication) have been defined and which has the properties of ordinary arithmetic, such as closure, associativity, commutativity, distributivity, and having both additive and multiplicative inverses.
- Finite fields are important in several areas of cryptography. A finite field is simply a field with a finite number of elements. It can be shown that the order of a finite field (number of elements in the field) must be a power of a prime \(p^n\), where \(n\) is a positive integer.
- Finite fields of order \(p\) can be defined using arithmetic mod \(p\).
- Finite fields of order \(p^n\), for \(n > 1\), can be defined using arithmetic over polynomials.
Groups

• Group G with operation \( \cdot \) obeys the following rules
  – Closure: if \( a \) and \( b \) belong to \( G \) then so does \( a \cdot b \)
  – Associativity: \( (a \cdot b) \cdot c = a \cdot (b \cdot c) \)
  – Identity: there is an identity element, call it \( e \), such that \( a \cdot e = e \cdot a = a \) for all elements \( a \) in \( G \)
  – Inverse: for every \( a \) in \( G \) there is an \( a' \) in \( G \) such that \( a \cdot a' = a' \cdot a = e \)

• An abelian group also obeys the commutative law: \( a \cdot b = b \cdot a \) for all \( a \) and \( b \) in \( G \)

• The set of integers \( \{ \ldots, -2, -1, 0, 1, 2, \ldots \} \) under addition is an example of an infinite abelian group
Group Work (no pun intended)

- Define the operation • by
- Is there closure? Why?
- Is • associative?
- Is there an identity element? What is it?
- Does every element have an inverse? What are the inverses of a and of b?
- Is • commutative? How can you tell?
- Can you think of an appropriate name for •?
Cyclic Group

• Exponentiation is repeated application of the group operator, such as $a \cdot a \cdot a \cdot a = a^4$

• A group is cyclic if every element can be expressed as a power of a particular element, call it $a$; that is, every element equals $a^k$ for some $k$

• We define $a^{-k}$ as $(a')^k$ and $a^0$ as the identity

• The element $a$ is a generator for the group

• For the set of integers under addition, $a = 1$, $a^k = 1 + 1 + \ldots + 1 = k$ and $a^0 = 0$

• $a' = -1$ so $a^{-k} = -1 + -1 + \ldots + -1 = -k$
Homework problem

• Consider $S_3$, all permutations of three elements
• Use the elements 1, 2, 3 write all possible permutations, label them using the scheme $a$ is 1 2 3, $b$ is 1 3 2, $c$ is 2 1 3, $d$ is 2 3 1, $e$ is 3 1 2 and $f$ is 3 2 1; clearly $a$ is the identity element
• Draw a composition table for permutations
• Is $S_3$ closed? Is it associative? Is there an identity element? Are there inverses?
• Is $S_3$ abelian? If not, give a counter example.
• Is $S_3$ a cyclic group?
Properties of a Ring

• A ring is a set $S$ with two operations we will call $+$ and $\times$, for convenience we write $\times$ using concatenation, so $a \times b$ is simply written $ab$
  – $(S, +)$ is an abelian group
  – $S$ is closed under $\times$, so $ab$ is in $S$ for all $a$ and $b$
  – The operation $\times$ is associative; how do we write this?
  – The distributive laws hold:
    $$a \times (b + c) = a \times b + a \times c \quad \text{and} \quad (a + b) \times c = a \times c + b \times c$$

• The ring is commutative if $a \times b = b \times a$ for all $a$ and $b$

• The set $S$ of even integers under addition and multiplication is a commutative ring
Group Work

• Given the operations + and \( x \) on \( S \) defined by

\[
\begin{array}{c|cc}
+ & a & b \\
\hline
a & a & b \\
b & b & a \\
\end{array}
\quad
\begin{array}{c|ccc}
\times & a & b \\
\hline
a & a & a \\
b & b & a \\
\end{array}
\]

• Is \( S \) a ring? Justify your answer.
• Is \( S \) a commutative ring? Justify.
Integral Domain

• An integral domain, call it $R$, is a commutative ring that obeys two additional properties
  – There is a multiplicative identity, call it $1$, such that $1 \cdot a = a \cdot 1 = a$ for all elements $a$ in $R$
  – No zero divisors: if $a$ and $b$ are in $R$ and $a \cdot b = 0$ then either $a = 0$ or $b = 0$

• The set of integers under addition and multiplication is an integral domain
A Field

• A field $F$ is an integral domain that satisfies one additional property
  – Assume the operations are $+$ and $\times$, the additive identity is 0 and the multiplicative identity is 1
  – For each $a$ in $F$, except 0, there is a multiplicative inverse $a^{-1}$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$

• In essence we are adding division since $a \cdot b^{-1} = a/b$

• The rational numbers, the real numbers, and the complex numbers are all fields

• Why isn’t the set of integers a field?

• We now turn our attention to finite groups, rings and fields
A Summary of Properties

Field

Integral domain

Commutative ring

Ring

Abelian group

Group

(A1) Closure under addition:
If $a$ and $b$ belong to $S$, then $a + b$ is also in $S$
a + (b + c) = (a + b) + c for all $a, b, c$ in $S$

(A2) Associativity of addition:

(A3) Additive identity:
There is an element $0$ in $R$ such that
$a + 0 = 0 + a = a$ for all $a$ in $S$

(A4) Additive inverse:
For each $a$ in $S$ there is an element $-a$ in $S$
such that $a + (-a) = (-a) + a = 0$

(A5) Commutativity of addition:
a + b = b + a for all $a, b$ in $S$

(M1) Closure under multiplication:
If $a$ and $b$ belong to $S$, then $ab$ is also in $S$
a(bc) = (ab)c for all $a, b, c$ in $S$

(M2) Associativity of multiplication:
a(b + c) = ab + ac for all $a, b, c$ in $S$

(M3) Distributive laws:
(a + b)c = ac + bc for all $a, b, c$ in $S$

(M4) Commutativity of multiplication:
ab = ba for all $a, b$ in $S$

(M5) Multiplicative identity:
There is an element $1$ in $S$ such that
$a1 = 1a = a$ for all $a$ in $S$

(M6) No zero divisors:
If $a, b$ in $S$ and $ab = 0$, then either
$a = 0$ or $b = 0$

(M7) Multiplicative inverse:
If $a$ belongs to $S$ and $a 
eq 0$, there is an
element $a^{-1}$ in $S$ such that $aa^{-1} = a^{-1}a = 1$
Modulo Arithmetic

• Integer division produces a quotient and remainder
  – a = qn + r where 0 <= r < n and q = \lfloor a/n \rfloor
  – The remainder is given by a mod n so
    a = \lfloor a/n \rfloor n + (a \mod n)
  – Find q and r for a = 43 and n = 9
  – Find q and r for a = -13 and n = 4

• Two integers are congruent modulo n
  – If (a \mod n) = (b \mod n) then we write a \equiv b \pmod n
  – Examples: 12 \equiv 27 \pmod 5 and -2 \equiv 19 \pmod 7
  – Modulo equality produces an infinite set, so the
    integers equal to 4 mod 7 are \{ \ldots -10, -3, 4, 11, 18 \ldots \}
Divisors

• We say $a|b$ if $a = mb$ for some integer $m$
  – the divisors of 30 are 1, 2, 3, 5, 6, 10, 15
  – If $a|1$ then $a = +1$ or $-1$
  – If $a|b$ and $b|a$ then $a = +b$ or $-b$
  – Any $b \neq 0$ divides 0
  – If $b|g$ and $b|h$ then $b|(mg + nh)$ for arbitrary integers $m,n$

• Properties of the modulo operator
  – $a \equiv b \mod n$ if $n|(a - b)$
  – $a \equiv b \mod n$ implies $b \equiv a \mod n$
  – $a \equiv b \mod n$ and $b \equiv c \mod n$ implies $a \equiv c \mod n$
Homework Problem

• How would you prove that mod is transitive? Namely, prove $a \equiv b \mod n$ and $b \equiv c \mod n$ implies $a \equiv c \mod n$.

• How would you get started?
Modulo Properties

- Properties
  - \[(a \mod n) + (b \mod n)] \mod n = (a + b) \mod n\]
  - \[(a \mod n) - (b \mod n)] \mod n = (a - b) \mod n\]
  - \[(a \mod n) \times (b \mod n)] \mod n = (a \times b) \mod n\]
  - How would you prove the last property?

- Examples
  - \[((12 \mod 5) + (13 \mod 5)) \mod 5 = [2 + 3] \mod 5 = 0 = (12 + 13) \mod 5\]
  - \[((12 \mod 5) \times (13 \mod 5)) \mod 5 = [2 \times 3] \mod 5 = 1 = (12 \times 13) \mod 5\]
  - \[7^4 \mod 8 \equiv (49)(49) \mod 8 \equiv 2401 \mod 8 \equiv 1 \mod 8\]
## Addition Modulo 8

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>×</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>2</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Residue Classes

• The entries in the previous tables are residue classes; each class represents an infinite set of integer values

• For example, the residue classes modulo 4 are
  
  \[ [0] = \{ \ldots, -12, -8, -4, 0, 4, 8, 12, \ldots \} \]
  \[ [1] = \{ \ldots, -11, -7, -3, 1, 5, 9, 13, \ldots \} \]
  \[ [2] = \{ \ldots, -10, -6, -2, 2, 6, 10, 14, \ldots \} \]
  \[ [3] = \{ \ldots, -9, -5, -1, 3, 7, 11, 15, \ldots \} \]

• The integers 0 through n-1 are used to represent their respective residue classes modulo n
  
  – Notice that these classes are mutually exclusive
  
  – The union of all these classes is the set of integers
Homework Problem

- Fill in the following tables for $\mathbb{Z}_5$

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\times$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Properties of $\mathbb{Z}_n$

<table>
<thead>
<tr>
<th>Property</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commutative laws</td>
<td>$(w + x) \mod n = (x + w) \mod n$</td>
</tr>
<tr>
<td></td>
<td>$(w \times x) \mod n = (x \times w) \mod n$</td>
</tr>
<tr>
<td>Associative laws</td>
<td>$\left[ (w + x) + y \right] \mod n = \left[ w + (x + y) \right] \mod n$</td>
</tr>
<tr>
<td></td>
<td>$\left[ (w \times x) \times y \right] \mod n = \left[ w \times (x \times y) \right] \mod n$</td>
</tr>
<tr>
<td>Distributive laws</td>
<td>$\left[ w \times (x + y) \right] \mod n = \left[ (w \times x) + (w \times y) \right] \mod n$</td>
</tr>
<tr>
<td></td>
<td>$\left[ w + (x \times y) \right] \mod n = \left[ (w + x) \times (w + y) \right] \mod n$</td>
</tr>
<tr>
<td>Identities</td>
<td>$(0 + w) \mod n = w \mod n$</td>
</tr>
<tr>
<td></td>
<td>$(1 \times w) \mod n = w \mod n$</td>
</tr>
<tr>
<td>Additive inverse ($-w$)</td>
<td>For each $w \in \mathbb{Z}_n$, there exists a $z$ such that $w + z \equiv 0 \mod n$</td>
</tr>
</tbody>
</table>
What about Multiplicative Inverses

• If \((ab) \equiv (ac) \pmod{n}\) can we conclude \(b \equiv c \pmod{n}\)?
  – In general the answer is no, consider
    \((6 \times 3) \equiv (6 \times 7) \pmod{8}\) since both \(\equiv 2\)
    but clearly 3 does not equal 7 mod 8
  – But in some cases it is true, as in
    \((5 \times 3) \equiv (5 \times 11) \pmod{8}\) since both \(\equiv 7\)
    and it is true 3 \(\equiv 11\) mod 8

• The conclusion above is only true if a and n are relatively prime
  – If \(\gcd(a, b) = 1\) then a and b are relative prime
  – The numbers relatively prime to 8 are 1, 3, 5, and 7
  – Notice that these numbers generate the entire group using exponentiation
Greatest Common Divisor

• Definition: \( c \) is the gcd\((a,b)\) if
  – \( c \) is a divisor of \( a \) and \( b \)
  – Any divisor of \( a \) and \( b \) is also a divisor of \( c \)
  – \( \gcd(a,b) = \max[k \text{ such that } k|a \text{ and } k|b] \)

• Some properties of gcd
  – \( \gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b) \)
  – So in general we can find \( \gcd(|a|,|b|) \)
  – \( \gcd(a,0) = |a| \)
  – As mentioned earlier if \( \gcd(a,b) = 1 \) then \( a \) and \( b \) are relatively prime
An important theorem

• \( \gcd(a, b) = \gcd(b, a \mod b) \)
  – The proof of this theorem is given in the textbook
  – This gives us a way to calculate the \( \gcd \) efficiently
  – \( \gcd(24, 18) = \gcd(18, 6) = \gcd(6, 0) = 6 \)
  – What if the order of the original numbers is reversed?
    – \( \gcd(18, 24) = \gcd(24, 18) = \gcd(18, 6) = \gcd(6, 0) = 6 \)
  – What if the numbers are relatively prime?
    – \( \gcd(80, 29) = \gcd(29, 22) = \gcd(22, 7) = \gcd(7, 1) = \gcd(1, 0) = 1 \)

• Euclid’s algorithm implements the process of finding the \( \gcd \) using this theorem
Euclid’s Algorithm

- **EUCLID**\((a,b)\)
  1. \(A \leftarrow a; B \leftarrow b\)
  2. If \(B = 0\) return \(A\)  // it is the \(\gcd(a,b)\)
  3. \(R = A \mod B\)
  4. \(A \leftarrow B\)
  5. \(B \leftarrow R\)
  6. Go to step 2

- An extended example
  \(\gcd(1970, 1066) = \gcd(1066, 904) = \gcd(904, 162) = \gcd(162, 94) = \gcd(94, 68) = \gcd(68, 26) = \gcd(26, 16) = \gcd(16, 10) = \gcd(10, 6) = \gcd(6, 4) = \gcd(4, 2) = \gcd(2, 0) = 2\)
Finite Fields of Order $p$

- Consider modular arithmetic order $p$
  - $p$ is a prime, meaning its only divisors are 1 and itself
  - All nonzero elements have a multiplicative inverse
  - Therefore, if $(a \times b) = (a \times c) \mod p$ then $b = c \mod p$

- A simple example, GF(2)

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$x$</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$w$</th>
<th>$-w$</th>
<th>$w^{-1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>__</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
### GF(7)

#### Addition Table

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

#### Multiplication Table

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Generator Elements

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
Extended Euclid

- Used to find the multiplicative inverse
- Extended Euclid(m,b)

1. \((A_1,A_2,A_3) \leftarrow (1,0,m); (B_1,B_2,B_3) \leftarrow (0,1,b)\)

2. If \(B_3 = 0\) return \(A_3 = \gcd(m,b); \) no inverse

3. If \(B_3 = 1\) return \(B_3 = \gcd(m,b); B_2\) is \(b^{-1}\)

4. \(Q = \text{floor}(A_3/B_3)\)

5. \((T_1,T_2,T_3) \leftarrow (A_1–Q \ B_1, A_2–Q \ B_2, A_3–Q \ B_3)\)

6. \((A_1,A_2,A_3) \leftarrow (B_1,B_2,B_3)\)

7. \((B_1,B_2,B_3) \leftarrow (T_1,T_2,T_3)\)

8. Goto step 2
Find the inverse of 5 in GF(17)

- We show the T’s too but as you can see they could have been written in the B’s columns

<table>
<thead>
<tr>
<th>Q</th>
<th>A1</th>
<th>A2</th>
<th>A3</th>
<th>B1</th>
<th>B2</th>
<th>B3</th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>1</td>
<td>0</td>
<td>17</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>-3</td>
<td>2</td>
<td>1</td>
<td>-3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>-3</td>
<td>2</td>
<td>-2</td>
<td>7</td>
<td>1</td>
<td>-2</td>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>

- So the inverse of 5 is 7
- Check \[ 5 \times 7 \equiv 1 \pmod{17} \]
- **Homework Problem**: find the inverse of 11
Polynomial Operations

\[ f(x) = \sum_{i=0}^{n} a_i x^i \quad g(x) = \sum_{i=0}^{m} b_i x^i \quad n \geq m \]

- **Addition**

\[ f(x) + g(x) = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i \]

- **Multiplication**

\[ f(x) \times g(x) = \sum_{i=0}^{m+n} c_i x^i \]

where \( c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0 \)
Polynomial Arithmetic in Galois Fields

• Polynomial arithmetic with coefficients in \( Z_p \)
  – This forms a polynomial ring
  – Division produces both a quotient and remainder
  – So objects may not have multiplicative inverses
  – We are particularly interested in \( Z_2 \)

• Looking ahead
  – We will look at polynomial arithmetic over GF(2\(^n\))
  – In this case objects do have multiplicative inverses
  – This results in a finite field
  – Modular polynomial arithmetic over GF(2\(^n\)) form a basis of the Advanced Encryption Standard (AES)
Polynomial Arithmetic over GF(2)

- GF(2) is important because arithmetic is easy
  - Addition is an XOR operation
  - Multiplication is an AND operation

- Here are some example operations; notice that the coefficients in GF(2) can only be 0 or 1 and that addition and subtraction give the same result

\[
\begin{align*}
x^7 &+ x^5 + x^4 + x^3 &+ x + 1 \\
+ (x^5 + x^4) &+ (x^3 + x + 1) \\
\hline
x^7 &+ x^5 + x^4
\end{align*}
\]
(a) Addition

\[
\begin{align*}
x^7 &+ x^5 + x^4 + x^3 &+ x + 1 \\
- (x^3 + x + 1) &- (x^3 + x + 1) \\
\hline
x^7 &+ x^5 + x^4
\end{align*}
\]
(b) Subtraction
Multiplication and Division

\[ \begin{array}{c}
  x^7 + x^5 + x^4 + x^3 + x + 1 \\
  \times (x^3 + x + 1) \\
  \hline
  x^7 + x^5 + x^4 + x^3 + x + 1 \\
  x^8 + x^6 + x^5 + x^4 + x^2 + x \\
  x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 \\
  \hline
  x^{10} + x^4 + x^2 + 1
\end{array} \]

\[ \begin{array}{c}
  x^3 + x + 1 \\
  \sqrt{x^7 + x^5 + x^4 + x^3 + x + 1} \\
  \hline
  x^7 + x^5 + x^4 \\
  \hline
  x^3 + x + 1 \\
  \hline
  x^3 + x + 1
\end{array} \]
Irreducible Polynomials

• Definition
  – A polynomial $f(x)$ is irreducible if and only if it cannot be expressed as a product of lower degree polynomials
  – These polynomials are also called prime polynomials

• Examples
  – $x^3 + 1$ is reducible since it equals $(x+1)(x^2+x+1)$
  – $x^3 + x^2 + 1$ is irreducible because if it was then one factor would have degree one and the other degree two
    • $x$ is clearly not a factor
    • $x + 1$ is not a factor because
      $x^3 + x^2 + 1 = x^2 (x + 1) + 1$
    • So there is no factor of degree one
GCD for polynomials

• \( \gcd(a(x), b(x)) = c(x) \) if
  – \( c(x) \) divides both \( a(x) \) and \( b(x) \)
  – Any divisor of \( a(x) \) and \( b(x) \) is a divisor of \( c(x) \)

• Euclid[\( a(x), b(x) \)]
  1. \( A(x) \leftarrow a(x); B(x) \leftarrow b(x) \)
  2. If \( B(x) = 0 \) then \( \gcd(a(x), b(x)) = A(x) \)
  3. \( R(x) = A(x) \mod B(x) \)
  4. \( A(x) \leftarrow B(x) \)
  5. \( B(x) \leftarrow R(x) \)
  6. Go to step 2
An Example

• Find \( \gcd(x^3+1, x^2+1) \) over GF(2)

\[
x^2 + 1 \overline{) x^3 + 1}
\]
\[
x^3 + x
\]
\[
x + 1
\]

\[
x + 1 \overline{) x^2 + 1}
\]
\[
x^2 + x
\]
\[
x + 1
\]
\[
\]
\[
x + 1
\]
\[
0
\]
Finite Fields of the Form GF($2^n$)

- **Desirable features**
  - Given appropriately defined structures (see next slide), operations produce a field; most importantly non-zero elements have inverses
  - Integers are mapped uniformly; here are the occurrences
    
    |     | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
    |-----|---|---|---|---|---|---|---|
    | $Z_8$ | 4 | 8 | 4 | 12| 4 | 8 | 4 |
    | GF($2^3$) | 7 | 7 | 7 | 7 | 7 | 7 | 7 |

  - Why is this important for cryptography; hint: with character to character ciphers and the uneven distribution of alphabetic characters in English words, a cipher is easily broken
Arithmetic in GF(2^3)

(a) Addition

<table>
<thead>
<tr>
<th></th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>000</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>001</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>010</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>6</td>
<td>7</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>011</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>100</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>101</td>
<td>5</td>
<td>4</td>
<td>7</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>110</td>
<td>6</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>111</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

(c) Additive and multiplicative inverses

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>5</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>7</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>7</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>7</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>7</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>

(b) Multiplication
Modular Polynomial Arithmetic

• Arithmetic operations
  – Follow the normal rules of algebra, refined by
  – Coefficient arithmetic is performed modulo $2^n$
  – If multiplication results in a polynomial with terms of
degree greater than $2^n - 1$, then the polynomial is
  reduced by some irreducible polynomial $m(x)$ of
degree $2^n$
  – This means we divide by $m(x)$ and keep the remainder

• A look ahead to AES
  – Polynomials are processed in $GF(2^8)$
  – $m(x)$ is $x^8 + x^4 + x^3 + x + 1$
Polynomials in $\text{GF}(2^3)$ mod $x^3 + x + 1$

- We need an irreducible polynomial of degree 3
  - There are two such polynomials, $x^3 + x + 1$ and $x^3 + x^2 + 1$; we choose the first one
  - It does not matter which one was chosen, since the resultant fields are isomorphic
- Question: what does “isomorphic” mean?

<table>
<thead>
<tr>
<th></th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000</td>
<td>0</td>
<td>1</td>
<td>x</td>
<td>x + 1</td>
<td>x^2</td>
<td>x^2 + 1</td>
<td>x^2 + x</td>
<td>x^2 + x + 1</td>
</tr>
<tr>
<td>001</td>
<td>1</td>
<td>0</td>
<td>x + 1</td>
<td>x</td>
<td>x^2 + 1</td>
<td>x^2</td>
<td>x^2 + x + 1</td>
<td>x^2 + x</td>
</tr>
<tr>
<td>010</td>
<td>x</td>
<td>x + 1</td>
<td>0</td>
<td>1</td>
<td>x^2 + x</td>
<td>x^2 + x + 1</td>
<td>x^2</td>
<td>x^2 + 1</td>
</tr>
<tr>
<td>011</td>
<td>x + 1</td>
<td>x</td>
<td>1</td>
<td>0</td>
<td>x^2 + x + 1</td>
<td>x^2 + x</td>
<td>x^2 + 1</td>
<td>x^2</td>
</tr>
<tr>
<td>100</td>
<td>x^2</td>
<td>x</td>
<td>x^2 + 1</td>
<td>x^2 + x</td>
<td>x^2 + x + 1</td>
<td>0</td>
<td>1</td>
<td>x</td>
</tr>
<tr>
<td>101</td>
<td>x^2 + 1</td>
<td>x^2</td>
<td>x^2 + x + 1</td>
<td>x^2 + x</td>
<td>1</td>
<td>0</td>
<td>x + 1</td>
<td>x</td>
</tr>
<tr>
<td>110</td>
<td>x^2 + x</td>
<td>x^2 + x + 1</td>
<td>x^2 + x</td>
<td>x^2 + 1</td>
<td>x</td>
<td>x + 1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>111</td>
<td>x^2 + x + 1</td>
<td>x^2 + x</td>
<td>x^2 + 1</td>
<td>x^2</td>
<td>x + 1</td>
<td>x</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

(a) Addition
**Polynomials in GF(2^3) mod x^3 + x + 1**

<table>
<thead>
<tr>
<th>×</th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>001</td>
<td>1</td>
<td>1</td>
<td>x</td>
<td>x + 1</td>
<td>x^2</td>
<td>x^2 + 1</td>
<td>x^2 + x</td>
<td>x^2 + x + 1</td>
</tr>
<tr>
<td>010</td>
<td>x</td>
<td>x</td>
<td>x^2</td>
<td>x^2 + x</td>
<td>x + 1</td>
<td>1</td>
<td>x^2 + x + 1</td>
<td>x^2 + 1</td>
</tr>
<tr>
<td>011</td>
<td>x + 1</td>
<td>x + 1</td>
<td>x^2 + x</td>
<td>x^2 + 1</td>
<td>x^2 + x + 1</td>
<td>1</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>100</td>
<td>x^2</td>
<td>x^2</td>
<td>x + 1</td>
<td>x^2 + x + 1</td>
<td>x^2 + x</td>
<td>x</td>
<td>x^2 + 1</td>
<td>1</td>
</tr>
<tr>
<td>101</td>
<td>x^2 + 1</td>
<td>x^2 + 1</td>
<td>1</td>
<td>x^2</td>
<td>x</td>
<td>x^2 + x + 1</td>
<td>x + 1</td>
<td>x^2 + x</td>
</tr>
<tr>
<td>110</td>
<td>x^2 + x</td>
<td>x^2 + x</td>
<td>x^2 + x + 1</td>
<td>1</td>
<td>x^2 + 1</td>
<td>x + 1</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>111</td>
<td>x^2 + x + 1</td>
<td>x^2 + x + 1</td>
<td>x^2 + 1</td>
<td>x</td>
<td>1</td>
<td>x^2 + x</td>
<td>x^2</td>
<td>x + 1</td>
</tr>
</tbody>
</table>

(b) **Multiplication**

- **Claim:** these two tables are equivalent
- **Try to explain why**
Yet Another Euclid’s Algorithm

- EXTENDED EUCLID\([m(x), b(x)]\]

1. \([A_1(x), A_2(x), A_3(x)] \leftarrow [1, 0, m(x)]\)
   \([B_1(x), B_2(x), B_3(x)] \leftarrow [0, 1, b(x)]\)
2. If \(B_3(x) = 0\) return \(A_3(x) = \gcd(m(x), b(x))\); no inverse
3. If \(B_3(x) = 1\) return \(B_3(x) = \gcd(m(x), b(x))\); \(B_2(x)\) is \(b^{-1}\)
4. \(Q(x) = \text{quotient of } A_3(x)/B_3(x)\)
5. \([T_1(x), T_2(x), T_3(x)] \leftarrow [A_1(x) - Q(x)B_1(x),\ 
   A_2(x) - Q(x)B_2(x), A_3(x) - Q(x)B_3(x)]\)
6. \([A_1(x), A_2(x), A_3(x)] \leftarrow [B_1(x), B_2(x), B_3(x)]\)
7. \([B_1(x), B_2(x), B_3(x)] \leftarrow [T_1(x), T_2(x), T_3(x)]\)
8. Goto step 2
A Sample Solution

- Find the inverse of $x^7 + x + 1 \mod x^8 + x^4 + x^3 + x + 1$
- The result is $x^7$

| Initialization | A1(x) = 1; A2(x) = 0; A3(x) = $x^8 + x^4 + x^3 + x + 1$
|                | B1(x) = 0; B2(x) = 1; B3(x) = $x^7 + x + 1$
| Iteration 1    | Q(x) = x
|                | A1(x) = 0; A2(x) = 1; A3(x) = $x^7 + x + 1$
|                | B1(x) = 1; B2(x) = x; B3(x) = $x^4 + x^3 + x^2 + 1$
| Iteration 2    | Q(x) = $x^3 + x^2 + 1$
|                | A1(x) = 1; A2(x) = x; A3(x) = $x^4 + x^3 + x^2 + 1$
|                | B1(x) = $x^3 + x^2 + 1$; B2(x) = $x^2 + 1$; B3(x) = x
| Iteration 3    | Q(x) = $x^3 + x^2 + x$
|                | A1(x) = $x^3 + x^2 + 1$; A2(x) = $x^2 + 1$; A3(x) = x
|                | B1(x) = $x^6 + x^2 + x + 1$; B2(x) = $x^7$; B3(x) = 1
| Iteration 4    | B3(x) = gcd([(x^7 + x + 1), ($x^8 + x^4 + x^3 + x + 1$)]) = 1
|                | B2(x) = $(x^7 + x + 1)^{-1} \mod (x^8 + x^4 + x^3 + x + 1) = x^7$
Computation in GF($2^8$)

- Addition is very simple, apply XOR $\oplus$

\[ (x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2 \]

is computed by

\[ (01010111) \oplus (10000011) = 11010100 \]

- Multiplication takes more work
  - We use $x^n \mod p(x) = [p(x) - x^n]$
  - In particular $x^8 \mod m(x) = x^4 + x^3 + x + 1$
  - Given any $f(x)$ we compute $x \times f(x) \mod m(x)$
  - Note that multiplying by $x$ is a one bit shift left
  - If $b_7 = 0$ then we are done
  - If $b_7 = 1$ we compute $(b_6b_5b_4b_3b_2b_1b_00) \oplus (00011011)$
Example Multiplication - 1

- Computing

\[(x^6 + x^4 + x^2 + x + 1) \times (x^7 + x + 1) = x^7 + x^6 + 1 \mod m(x)\]

  - First find \((01010111)\) times the powers of \(x\)
  - \((01010111) \times (00000010) = (10101110) \quad \text{// times } x\)
  - \((01010111) \times (00000100) =\)
    \[(01011100) \oplus (00011011) = (01000111) \quad \text{// times } x^2\]
  - \((01010111) \times (00001000) = (10001110) \quad \text{// times } x^3\)
  - \((01010111) \times (00010000) =\)
    \[(00011100) \oplus (00011011) = (00000111) \quad \text{// times } x^4\]
  - \((01010111) \times (00100000) = (00001110) \quad \text{// times } x^5\)
  - \((01010111) \times (01000000) = (00011100) \quad \text{// times } x^6\)
  - \((01010111) \times (10000000) = (00111000) \quad \text{// times } x^7\)
Example Multiplication – 2

• Now we do the multiply
  – \((01010111) \times (10000011) = (01010111) \times (1000000) \oplus (00000010) \oplus (00000001)\)
  – Using distribution & the results from the previous slide
    \(= (00111000) \oplus (10101110) \oplus (01010111)\)
    \(= 11000001\)
• Translating back into polynomial notation the result is \(x^7 + x^6 + 1\)
• Although polynomial arithmetic looks intimidating, when performed in binary it can be computed very efficiently
• **Homework Problem**
  \((x^7 + x^5 + x^2 + x + 1) \times (x^6 + x^2 + 1) \mod x^3 + x + 1\)