Divisibility, Primes

- **Definition.** $\mathbb{N}$ denotes the set \{1, 2, 3, \ldots\} of **natural numbers** and $\mathbb{Z}$ denotes the set of **integers** \{\ldots, −2, −1, 0, 1, 2, \ldots\}. $\mathbb{R}$ denotes the **real numbers** and $\mathbb{C}$ denotes the complex numbers.

- **Definition.** The integer $n$ is **divisible** by the integer $d$, denoted by $d \mid n$, if $a \cdot d = n$ for some integer $a$.

- **Definition.** A positive integer $p$, $p > 1$, is called a **prime** if it is divisible only by $\pm p$ and $\pm 1$. Any integer greater than 1 which is not prime is called **composite**.

- **Theorem.** (Euclid, 300 B.C.) There are infinitely many primes.

- **Proof.** Assume that the set of primes is finite, e.g., $\{p_1, p_2, \ldots, p_n\}$. Then the integer $N = 1 + p_1 p_2 \cdots p_n$ is not divisible by any of the primes $p_1, \ldots p_n$. 
Prime Numbers

- Between any two primes there can be arbitrarily large gaps. For instance, the sequence $n! + 2, n! + 3, \ldots n! + n$ contains $n - 1$ consecutive composite numbers.

- Definition. The prime counting function $\pi(x)$ is defined by
  \[ \pi(x) = |\{p \text{ prime} | p \leq x\}|, \]
  i.e., $\pi(x)$ is equal to the number of primes less than or equal to $x$.

- Example: $\pi(50) = 15$ since
  \[ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 \]
  are all primes $p \leq 50$.

- **Prime Number Theorem.** (Hadamard, de la Vallée Poussin, 1896) $\pi(x)$ satisfies
  \[ \lim_{x \to \infty} \frac{\pi(x) \ln(x)}{x} = 1 \quad \implies \quad \pi(x) \approx \frac{x}{\ln x}. \]
Example

Using $\pi(x) \approx x/\ln x$, the number of primes with $n$ decimal digits is

$$\pi(10^n) - \pi(10^{n-1}) \approx \frac{9n - 1}{n(n - 1)} \cdot 10^{n-1} \log_{10} e \approx \frac{10^n}{3n}.$$

Approximate numerical values are

<table>
<thead>
<tr>
<th>$n$</th>
<th>bits</th>
<th>$\pi(10^n) - \pi(10^{n-1})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>128</td>
<td>$\approx 3.5 \times 10^{36}$</td>
</tr>
<tr>
<td>77</td>
<td>256</td>
<td>$\approx 5.9 \times 10^{74}$</td>
</tr>
<tr>
<td>100</td>
<td>332</td>
<td>$\approx 3.9 \times 10^{97}$</td>
</tr>
<tr>
<td>154</td>
<td>512</td>
<td>$\approx 3.4 \times 10^{151}$</td>
</tr>
<tr>
<td>308</td>
<td>1024</td>
<td>$\approx 1.9 \times 10^{305}$</td>
</tr>
<tr>
<td>617</td>
<td>2048</td>
<td>$\approx 1.7 \times 10^{613}$</td>
</tr>
</tbody>
</table>

As can be seen, there is no shortage for the number of primes with $n$ digits.
Greatest Common Divisor

- **Definition:** The *greatest common divisor* of two integers $n_1$ and $n_2$, denoted $\gcd(n_1, n_2)$, is the largest positive integer that divides both $n_1$ and $n_2$.

- **Definition:** If $\gcd(n_1, n_2) = 1$, then $n_1$ and $n_2$ are said to be *relatively prime*.

- **Example:** *Fermat’s (little) theorem* states that for $p$ prime

  $$ p \mid (a^{p-1} - 1), \quad \text{if } \gcd(a, p) = 1, $$

  e.g., 5 divides $3^4 - 1 = 80$, or 7 divides $2^6 - 1 = 63$.

- **Definition:** The *least common multiple* of two integers $n_1$ and $n_2$, denoted $\text{lcm}(n_1, n_2)$, is the smallest positive integer divisible by both $n_1$ and $n_2$. 

Peter Mathys
ECEN 5022 Cryptography
Division Algorithm

▶ **Theorem: Division Algorithm.** Given a pair of integers, \( c \) and \( d \neq 0 \), there is a unique pair of integers \( q \) and \( r \), called *quotient* and *remainder*, such that

\[
c = q \cdot d + r, \quad 0 \leq r < |d|.
\]

▶ **Proof:** Assume that there are two solutions, i.e.,
\[
c = q_1 \cdot d + r_1 = q_2 \cdot d + r_2, \text{ with } 0 \leq r_1 < |d| \text{ and } 0 \leq r_2 < |d|.
\]
Thus, \((q_1 - q_2) \cdot d = r_2 - r_1\) and \(-|d| < r_2 - r_1 < |d|\). But since \( r_2 - r_1 \) must be a multiple of \( d \), this implies that \( r_2 - r_1 = 0 \). Since \( d \neq 0 \), this also implies that \( q_1 - q_2 = 0 \) and thus \( q \) and \( r \) are unique. \( \text{QED} \)
Remainders

Definition: The notation

\[ r = R_d(c), \]

means that \( r \) is the remainder of \( c \) when divided by \( d \).

Note: Another notation that is often used in connection with remainders is

\[ r \equiv c \pmod{d}. \]

This means that “\( r \) is congruent to \( c \) modulo \( d \)”. In this case \( 0 \leq r < |d| \) is not guaranteed and thus \( r \) is not unique. For example, \( 9 \equiv 16 \pmod{7} \) as well as \( 2 \equiv 16 \pmod{7} \).

Theorem: Computations with remainders satisfy

(i) \[ R_d(a + b) = R_d(R_d(a) + R_d(b)). \]

(ii) \[ R_d(a \cdot b) = R_d(R_d(a) \cdot R_d(b)). \]

Proof: Left as an exercise.
Euclid’s Algorithm

Euclid’s Algorithm. The greatest common divisor, \( \gcd(n_1, n_2) \), of two integers \( n_1, n_2, n_2 \neq 0 \), is computed by repeated application of the division algorithm as follows:

\[
\begin{align*}
  n_1 &= q_2 n_2 + n_3 \\
  n_2 &= q_3 n_3 + n_4 \\
  &\vdots \\
  n_{m-2} &= q_{m-1} n_{m-1} + n_m \\
  n_{m-1} &= q_m n_m + 0 .
\end{align*}
\]

The process stops when a zero remainder is obtained. The last nonzero remainder is the desired result, i.e., \( \gcd(n_1, n_2) = n_m \).

Proof: Sketch. Use the fact that \( \gcd(n_1, n_2) = \gcd(n_1 + kn_2, n_2) \), for any integer \( k \).
Euclid’s Extended Algorithm

**Corollary:** For any integers \( n_1 \) and \( n_2 \neq 0 \) there exist integers \( a \) and \( b \) such that

\[
\gcd(n_1, n_2) = a n_1 + b n_2.
\]

That is, \( \gcd(n_1, n_2) \) can be expressed as a linear combination of \( n_1 \) and \( n_2 \).

**Proof:** Use Euclid’s algorithm, starting with the last equation and work backwards to the first equation, to compute

\[
\begin{align*}
\gcd(n_1, n_2) &= n_m = n_{m-2} - q_{m-1} n_{m-1} \\
n_{m-1} &= n_{m-3} - q_{m-2} n_{m-2} \\
&\vdots \\
n_3 &= n_1 - q_2 n_2.
\end{align*}
\]

Then successively eliminate all the intermediate remainders \( n_{m-1}, n_{m-2}, \ldots, n_3 \), to obtain \( \gcd(n_1, n_2) \) as a linear combination of \( n_1 \) and \( n_2 \) with integer coefficients. QED
Euclid’s Algorithm for \( \text{gcd} \)

**START**

Initialize
\[
i \leftarrow 2
\]
\[
a_1 \leftarrow 1, \; b_1 \leftarrow 0
\]
\[
a_2 \leftarrow 0, \; b_2 \leftarrow 1
\]

Input \( n_1, n_2 \)

\[
q \leftarrow \left\lfloor \frac{n_{i-1}}{n_i} \right\rfloor
\]
\[
n_{i+1} \leftarrow n_{i-1} - q n_i
\]

\[\text{no} \quad n_{i+1} = 0? \]

\[
i \leftarrow i + 1
\]
\[
a_i \leftarrow a_{i-2} - q a_{i-1}
\]
\[
b_i \leftarrow b_{i-2} - q b_{i-1}
\]

\[\text{yes} \quad \text{Output } n_i, a_i, b_i
\]
\[
n_i = \text{gcd}(n_1, n_2)
\]
\[
= a_i n_1 + b_i n_2
\]

**STOP**
Groups, Rings, Fields

- Over the reals \( \mathcal{R} \) (or rationals \( \mathcal{Q} \) or complex number \( \mathcal{C} \)) one can add, subtract, multiply, and divide.
- Over the integers \( \mathcal{Z} \) one can add, subtract, and multiply.
- **Group:** Set of mathematical objects for which “addition” and “subtraction” are defined.
- **Ring:** Set of mathematical objects for which “addition”, “subtraction” and “multiplication” are defined.
- **Field:** Set of mathematical objects for which “addition”, “subtraction”, “multiplication” and “division” are defined.
- Note: “addition”, “subtraction”, “multiplication” and “division” are not necessarily the usual ‘+’, ‘−’, ‘×’ and ‘÷’.
Some Definitions

▶ **Definition:** A set $S$ is an arbitrary collection of elements, without any predefined operations between the set elements.

▶ **Definition:** The *cardinality* $|S|$ of a set $S$ is the number of objects in the set. $|S|$ can be *finite*, *countably infinite*, or *uncountably infinite*.

▶ **Examples:** The set of tea cups in a kitchen cabinet is a finite set. The set $\mathbb{Q}$ of rational numbers is countably infinite. The set $\mathbb{R}$ of real numbers is uncountably infinite.
Axioms

Let $S$ denote a set of mathematical objects. For any $a, b, c \in S$ define the following axioms:

(A.1) $a + b \in S$

(A.2) $a + (b + c) = (a + b) + c = a + b + c$

(A.3) $a + 0 = 0 + a = a$, $0 \in S$

(A.4) $a + (-a) = (-a) + a = 0$, $(-a) \in S$

(A.5) $a + b = b + a$

(B.1) $a \cdot b \in S$

(B.2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$

(B.3) $a \cdot 1 = 1 \cdot a = a$, $1 \in S \setminus \{0\}$

(B.4) $a \cdot (a^{-1}) = (a^{-1}) \cdot a = 1$, $a, (a^{-1}) \in S \setminus \{0\}$

(B.5) $a \cdot b = b \cdot a$

(C.1) $(a + b) \cdot c = a \cdot c + b \cdot c$

Closure wrt $+$

Associativity wrt $+$

Identity element wrt $+$

Inverse element wrt $+$

Commutativity wrt $+$

Closure wrt $\cdot$

Associativity wrt $\cdot$

Identity element wrt $\cdot$

Inverse element wrt $\cdot$

Commutativity wrt $\cdot$

Distributivity
## Groups, Rings, Fields

- Depending on the subset of axioms that are satisfied the following arithmetic systems are defined:

<table>
<thead>
<tr>
<th>Axioms satisfied</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A.1)...(A.4)</td>
<td>Group</td>
</tr>
<tr>
<td>(A.1)...(A.4),(A.5)</td>
<td>Commutative Group</td>
</tr>
<tr>
<td>(A.1)...(A.5),(B.1)...(B.3),(C.1)</td>
<td>Ring with Identity</td>
</tr>
<tr>
<td>(A.1)...(A.5),(B.1)...(B.3),(B.5),(C.1)</td>
<td>Commutative Ring with Identity</td>
</tr>
<tr>
<td>(A.1)...(A.5),(B.1)...(B.5),(C.1)</td>
<td>Field</td>
</tr>
</tbody>
</table>

- Note: *Commutative* groups (rings, fields) are also called *Abelian* groups (rings, fields) in honor of Niels Henrik Abel (1802-1829).
Notation, Definitions

Notation:

- A **group** with set of elements $G$ and operation ‘$\ast$’ is denoted by $\langle G, \ast \rangle$.
- A **ring** with set of elements $R$ and operations ‘$+$’ and ‘$\cdot$’ is denoted by $\langle R, +, \cdot \rangle$.
- A **field** with set of elements $F$ and operations ‘$+$’ and ‘$\cdot$’ is denoted by $\langle F, +, \cdot \rangle$.

Example: The set of all permutations of $n$ objects forms a (generally non-commutative) group under the operation of concatenation of permutations.

Example: The set of all binary $2 \times 2$ matrices forms a non-commutative ring with identity under the operations of binary (i.e., modulo 2) matrix addition and binary matrix multiplication. This ring has 16 elements.

Example: The set of all polynomials in the indeterminate $x$ with real coefficients form a commutative ring with identity. This ring has an infinite number of elements.
Finite Groups, Rings, Fields

- **Definition:** If $|G|$ (or $|R|$ or $|F|$) is finite then $<G, \ast>$ is called a *finite* group (or $<R, +, \cdot>$ is called a *finite* ring, $<F, +, \cdot>$ is called a *finite* field).

- **Definition:** A finite field with $q$ elements is denoted by GF$(q)$, where GF stands for Galois field in honor of Évariste Galois (1811-1832).

- **Theorem: Finite Fields.**
  
  (i) If $F$ is a finite field then $F$ contains $p^m$ elements for some prime $p$ and integer $m \geq 1$.
  
  (ii) For every prime power $p^m$ there is a unique (up to isomorphism) finite field of order $p^m$, called GF$p^m$ or $\mathbb{F}_{p^m}$
Finite Groups, Rings, Fields

Example: The integers 0, 1, \ldots, 6 form the finite field $\mathbb{GF}(7)$ under the operations of addition and multiplication modulo 7. Here are the group operation tables for $\mathbb{GF}(7)$:

\begin{align*}
\begin{array}{c|cccccccc}
+ & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
0 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
1 & 1 & 2 & 3 & 4 & 5 & 6 & 0 \\
2 & 2 & 3 & 4 & 5 & 6 & 0 & 1 \\
3 & 3 & 4 & 5 & 6 & 0 & 1 & 2 \\
4 & 4 & 5 & 6 & 0 & 1 & 2 & 3 \\
5 & 5 & 6 & 0 & 1 & 2 & 3 & 4 \\
6 & 6 & 0 & 1 & 2 & 3 & 4 & 5 \\
\end{array}
\quad
\begin{array}{c|cccccccc}
\times & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
2 & 0 & 2 & 4 & 6 & 1 & 3 & 5 \\
3 & 0 & 3 & 6 & 2 & 5 & 1 & 4 \\
4 & 0 & 4 & 1 & 5 & 2 & 6 & 3 \\
5 & 0 & 5 & 3 & 1 & 6 & 4 & 2 \\
6 & 0 & 6 & 5 & 4 & 3 & 2 & 1 \\
\end{array}
\end{align*}
More Definitions

- **Definition:** The elements in a ring with identity which have an inverse with respect to the second operation are called *units*.

- **Example:** The ring which is obtained by adding and multiplying integers modulo 10 has units 1, 3, 7, and 9.

- **Definition:** Let \(<G, \ast>\) be a group and let \(H\) be a nonempty subset of \(G\). Then \(H\) is called a *subgroup* of \(G\) if \(<H, \ast>\) is a group.

- **Example:** In the group of non-zero integers under the operation of multiplication modulo 7, the set of elements \(\{1, 2, 4\}\) forms a subgroup. Another subgroup is formed by the set of elements \(\{1, 6\}\).
More Definitions

Definition: Let \( <R, +, \cdot> \) be a ring and let \( H \) be a nonempty subset of \( R \). Then \( H \) is called a subring of \( R \) if \( <H, +, \cdot> \) is a ring.

Note: In particular, identity with respect to the first operation must be in \( H \) and closure must hold (under all specified operations) for elements in \( H \).

Definition: Let \( <E, +, \cdot> \) be a field. Then \( F \subset E \) is called a subfield of \( E \) if \( <F, +, \cdot> \) is a field. The field \( E \) is called an extension field of \( F \).

Example: Consider the field of rational numbers \( \mathbb{Q} \), the field of real numbers \( \mathbb{R} \), and the field of complex numbers \( \mathbb{C} \). Then \( \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \), and \( \mathbb{Q} \) is called a subfield of \( \mathbb{R} \) and \( \mathbb{C} \) is called an extension field of \( \mathbb{R} \).
Isomorphism

Definition: Isomorphism. Two groups $<G, +>$ and $<G', \ast>$ are isomorphic if a one-to-one mapping $f(.)$ exists such that

(i) $a' = f(a)$ (and thus $a = f^{-1}(a')$) for all $a \in G$ and $a' \in G'$,
(ii) if $a' = f(a)$, $b' = f(b)$, then

$$a' \ast b' = f(a + b) \quad \text{(and thus } a + b = f^{-1}(a' \ast b'))$$

for any $a, b \in G$ (or any $a', b' \in G'$).

That is, there has to be a one-to-one correspondence between the elements of the two groups which is preserved under the group operations ‘+’ and ‘∗’.

Note: Isomorphism for rings and fields is defined analogously. In this case the one-to-one correspondence must be preserved for both operations of the rings/fields.
Subgroups

To obtain a subgroup $H$ of a finite group $G$, one can proceed as follows. Take any $h \in G$ and let $H$ be the set 
\[ \{ h, h \times h, h \times h \times h, \ldots \} , \]
or, using a more concise notation,
\[ H = \{ h, h^2, h^3, \ldots, h^c = 1 \} , \]
where $c$, called the order of $H$, is the smallest positive integer such that $h^c = 1$.

**Example:** Consider the group $G = \{ 1, 2, \ldots, 12 \}$ of integers under the operation of multiplication modulo 13. Starting from $h = 5$, the set
\[ H = \{ 5^1 = 5, 5^2 = 12, 5^3 = 8, 5^4 = 1 \} , \]
is obtained, which forms a subgroup of $G$ of order 4.
Theorem: If \( G \) is a finite group and \( h \in G \), then a smallest positive integer \( c \), called the order of the element \( h \), exists such that \( h^c = 1 \). Moreover, the first element in the sequence \( h, h^2, h^3, \ldots \) which is repeated is \( h \) itself.

Proof: The element \( h \) is a member of a finite group and thus a repetition must eventually occur in \( h, h^2, h^3, \ldots \), that is, there must be two positive integers \( k, m, m > k \), such that \( h^k = h^m \). Since \( h^{-k} \) must be an element of \( G \), one can write

\[
1 = h^k \cdot h^{-k} = h^m \cdot h^{-k} = h^{m-k},
\]

which proves that there is at least one positive integer \( c \) such that \( h^c = 1 \). But then \( h^{c+1} = h \) and, since \( h, h^2, \ldots, h^c \) must all be distinct (otherwise \( c \) is not smallest positive integer such that \( h^c = 1 \)), \( h \) is the first element which is repeated. QED
(Sub)Groups

- **Definition:** \( h, h^2, h^3, \ldots, h^c = 1 \) is called a *cycle*.

- **Note:** A cycle is a subgroup.

- **Definition:** A group that consists of all the powers of one of its elements, say, \( \alpha \), is called a *cyclic group* (i.e., \( G = \{ \alpha, \alpha^2, \ldots, \alpha^c = 1 \} \)). The element \( \alpha \) is called a *primitive element* or a *generator* of the group.

- **Example:** Let \( <G, \cdot> \) be the set of integers under multiplication modulo 13. Then, choosing \( \alpha = 2 \),

\[
\begin{align*}
\alpha^0 &= 1 & \alpha^4 &= 3 & \alpha^8 &= 9 & \alpha^{12} &= 1 \\
\alpha^1 &= 2 & \alpha^5 &= 6 & \alpha^9 &= 5 \\
\alpha^2 &= 4 & \alpha^6 &= 12 & \alpha^{10} &= 10 \\
\alpha^3 &= 8 & \alpha^7 &= 11 & \alpha^{11} &= 7 \\
\end{align*}
\]

Thus, \( <G, \cdot> \) is a cyclic group and \( \alpha = 2 \) is a primitive element in this group.
Generator of a Group

▶ **Definition:** *Generator of a group.* A subset $X$ of a group $\langle G, * \rangle$ is called a *generator* if every element of $G$ can be expressed in the form $x_i * x_j * \ldots$. If $X$ is a finite set, then $G$ is said to be *finitely generated.*

▶ **Example:** $X = \{2\}$ is a generator of the group of integers under modulo 13 multiplication.

▶ **Example:** $X = \{2, 11\}$ is a generator of the group of integers $\{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15. Note that this group is not cyclic.
Coset Decomposition of a Group

Definition: Coset Decomposition of finite group with respect to subgroup. A finite group \( <G, *> \) can be decomposed with respect to a subgroup \( <H, *> \) as follows:

\[
\begin{align*}
  h_1 &= 1 \\
  g_2 * h_1 &= g_2 \\
  g_3 * h_1 &= g_3 \\
  \vdots & \quad \vdots \\
  g_m * h_1 &= g_m \\
  g_2 * h_2 &= g_2 \\
  g_3 * h_2 &= g_3 \\
  \vdots & \quad \vdots \\
  g_m * h_2 &= g_m \\
  g_2 * h_3 &= g_2 \\
  g_3 * h_3 &= g_3 \\
  \vdots & \quad \vdots \\
  g_m * h_3 &= g_m \\
  & \quad \vdots \\
  g_2 * h_n &= g_2 \\
  g_3 * h_n &= g_3 \\
  \vdots & \quad \vdots \\
  g_m * h_n &= g_m
\end{align*}
\]

The rows of the coset decomposition are called cosets. The first row is the subgroup \( H \). The elements \( h_1, g_2, g_3, \ldots, g_m \) in the first column are called coset leaders.
Coset Decomposition of a Group

- In general the construction of the coset decomposition proceeds as follows:
  - Start with the elements of $H$ in the first row (each element occurs exactly once).
  - Then choose an (arbitrary) element of $G$ which has not yet appeared in the table as coset leader and complete the corresponding coset. Repeat this step until all elements of $G$ are used.

- Note that the array constructed in this way is always rectangular and the construction always stops since $G$ is finite. For non-Abelian groups left coset decompositions with elements $g_i \ast h_j$ are distinguished from right coset decompositions with elements $h_j \ast g_i$. 

Coset Decomposition of a Group

▶ **Theorem:** Every element of $G$ appears exactly once in a coset decomposition of $G$.

▶ **Proof:** omitted.

▶ **Corollary:** If $H$ is a subgroup of $G$, then $|H|$ divides $|G|$.

▶ **Proof:** Follows from the rectangular structure of the coset decomposition.

▶ **Theorem: Lagrange.** The order of a finite group is divisible by the order of any of its elements.

▶ **Proof:** The group contains the cyclic subgroup generated by any element of the group. The above corollary thus proves the theorem.
Ring of Integers Modulo $n$

- **Definition:** $\mathbb{Z}_n$ denotes the ring of integers modulo $n$ with operations $+$ (addition mod $n$) and $\cdot$ (multiplication mod $n$). The elements of $\mathbb{Z}_n$ are $0, 1, \ldots, n-1$.

- **Definition:** The set of residues modulo $n$ that are relatively prime to $n$ is denoted $\mathbb{Z}_n^*$. Since any $a \in \mathbb{Z}_n^*$ satisfies $\gcd(a, n) = 1$, $a^{-1}$ exists and thus $\mathbb{Z}_n^*$ forms an Abelian group under multiplication modulo $n$. The elements $a \in \mathbb{Z}_n^*$ are the *units* of $\mathbb{Z}_n$. 

Peter Mathys
ECEN 5022 Cryptography
Euler’s Totient Function

Definition: Euler’s Totient Function $\phi$. Euler’s totient function, $\phi(n)$, evaluated at a positive integer $n$, is given by

$$\phi(n) = |\{0 \leq r < n | \gcd(r, n) = 1\}|,$$

i.e., it is the number of integers in the set $\{0, 1, 2, \ldots, n-1\}$ that are relatively prime to $n$. By definition, $\phi(1) = 1$.

Euler’s totient function can be computed as follows. Assume that $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the factorization of $n$ into distinct prime powers. Then

$$\phi(n) = \prod_{i=1}^{m} p_i^{e_i-1} (p_i - 1) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right).$$
Euler’s Totient Function

Note that if $gcd(n_1, n_2) = 1$, then $\phi(n_1 n_2) = \phi(n_1) \phi(n_2)$, and thus

$$\phi(n) = \phi(p_1^{e_1}) \phi(p_2^{e_2}) \cdots \phi(p_m^{e_m}),$$

where $\phi(p_i^{e_i}) = p_i^{e_i - 1} (p_i - 1)$. Note that this also implies that $\phi(n) \geq 1$.

**Theorem:** The order of the group $\mathbb{Z}_n^*$ is $\phi(n)$.

**Proof:** Follows directly from the definition of Euler’s totient function $\phi(n)$. QED
Euler’s Theorem

Theorem: Euler’s Theorem. If \( a \in \mathbb{Z}_n^* \), then

\[
a^{\phi(n)} = 1 \pmod{n}.
\]

Proof: The elements \( \{r_1, r_2, \ldots, r_m\} \) of \( \mathbb{Z}_n^* \) are all integers

\( 0 < r < n \) such that \( \gcd(r, n) = 1 \) and thus \( |\mathbb{Z}_n^*| = \phi(n) = m \).

For each \( i, 1 \leq i \leq m \), there is a unique \( j, 1 \leq j \leq m \) such

that \( ar_i = r_j \pmod{n} \). Since both \( a \) and \( r_i \) are relatively prime

to \( n \), \( ar_i \) is also relatively prime to \( n \) and thus

\[
\begin{align*}
\underbrace{ar_1 \cdot ar_2 \cdots ar_m} & \equiv r_1 \cdot r_2 \cdots r_m \pmod{n} \\
& = a^m (r_1 \cdot r_2 \cdots r_m)
\end{align*}
\]

This implies that \( (a^m - 1) r_1 \cdot r_2 \cdots r_m = 0 \pmod{n} \) and

because of \( \gcd(r_i, n) = 1 \) for all \( i \) it follows that

\( a^m = a^{\phi(n)} = 1 \pmod{n} \).

QED
Fermat’s Little Theorem

▶ **Corollary: Fermat’s Little Theorem.** Suppose \( p \) is a prime and \( a \in \mathbb{Z}_p^* \). Then

\[
a^{p-1} = 1 \pmod{p}.
\]

▶ **Proof:** \( \mathbb{Z}_p^* \) is a multiplicative group of order \( \phi(p) = p - 1 \).

QED
Chinese Remainder Theorem

Theorem: (The Chinese Remainder Theorem.) Given \( n_1, n_2, \ldots, n_k \) such that \( \gcd(n_i, n_j) = 1 \) for \( i \neq j \), the set of simultaneous congruences

\[
  x = a_i \pmod{n_i}, \quad i = 1, 2, \ldots, k,
\]

has a unique solution \( x \) modulo \( N = n_1 n_2 \cdots n_k \).

Proof: Define \( N_i = N/n_i \). Note that \( \gcd(N_i, n_i) = 1 \). Thus, using Euclid’s extended algorithm,

\[
  \gcd(N_i, n_i) = 1 = M_i N_i + m_i n_i \quad \implies \quad M_i N_i = 1 \pmod{n_i}.
\]

Therefore, the desired solution is

\[
  x = a_1 M_1 N_1 + a_2 M_2 N_2 + \ldots + a_k M_k N_k \pmod{N}.
\]

Check: \( x = a_i M_i N_i = a_i \pmod{n_i} \).
**Chinese Remainder Theorem**

► **Proof:** (contd.) To prove uniqueness of the solution, suppose that \( x \) and \( x' \) are two different solutions satisfying

\[
x = a_i \pmod{n_i}, \quad i = 1, 2, \ldots, k,
\]
\[
x' = a_i \pmod{n_i}, \quad i = 1, 2, \ldots, k.
\]

Then

\[
\Delta = x - x' = 0 \pmod{n_i}, \quad i = 1, 2, \ldots, k.
\]

Thus, \( \Delta \) is divisible by \( n_1, n_2, \ldots, n_k \). Since \( \gcd(n_i, n_j) = 1 \) for \( i \neq j \), \( \Delta \) must satisfy

\[
\Delta = m N, \quad m \text{ integer}, \quad N = n_1 n_2 \cdots n_k,
\]

which implies \( \Delta = 0 \pmod{N} \). QED
Chinese Remainder Theorem

Example: $n_1 = 3$, $n_2 = 4$, $n_3 = 5$, and thus $N = 60$, $N_1 = 60/3 = 20$, $N_2 = 60/4 = 15$, and $N_3 = 60/5 = 12$. Suppose that

$$x = 2 \pmod{3}, \quad x = 1 \pmod{4}, \quad x = 4 \pmod{5}.$$ 

Compute the quantities

$$\text{gcd} (N_1, n_1) = \text{gcd} (20, 3) = 1 = -1 \cdot 20 + 7 \cdot 3 \implies M_1 = -1 = 2 \pmod{3},$$
$$\text{gcd} (N_2, n_2) = \text{gcd} (15, 4) = 1 = -1 \cdot 15 + 4 \cdot 4 \implies M_2 = -1 = 3 \pmod{4},$$
$$\text{gcd} (N_3, n_3) = \text{gcd} (12, 5) = 1 = -2 \cdot 12 + 5 \cdot 5 \implies M_3 = -2 = 3 \pmod{5}.$$

The solution $x$ is then obtained as

$$x = 2 \cdot 2 \cdot 20 + 1 \cdot 3 \cdot 15 + 4 \cdot 3 \cdot 12 = 80 + 45 + 144 = 269 = 29 \pmod{60}.$$ 

Check:

$$29 = 2 \pmod{3}, \quad 29 = 1 \pmod{4}, \quad 29 = 4 \pmod{5}.$$
Quadratic Residues

Definition: An element $x \in \mathbb{Z}_n^*$ is called a quadratic residue modulo $n$ ($QR_n$) if $x = y^2 \pmod{n}$ for some $y \in \mathbb{Z}_n^*$. Otherwise, if no such $y \in \mathbb{Z}_n^*$ exists, $x$ is called a quadratic non-residue modulo $n$ ($QNR_n$).

Note: If $x \in QR_n$ then an element $y$ exists such that $\sqrt{x} = y \pmod{n}$.

Example: If $n = 13$ (prime)

<table>
<thead>
<tr>
<th>$y$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>$y^2$</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>3</td>
<td>12</td>
<td>10</td>
<td>10</td>
<td>12</td>
<td>3</td>
<td>9</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Thus, $QR_{13} = \{1, 3, 4, 9, 10, 12\}$, and $QNR_{13} = \{2, 5, 6, 7, 8, 11\}$ and

$\sqrt{1} = \pm 1 \pmod{13}$, $\sqrt{3} = \pm 4 \pmod{13}$, $\sqrt{4} = \pm 2 \pmod{13}$, $\sqrt{9} = \pm 3 \pmod{13}$, $\sqrt{10} = \pm 6 \pmod{13}$, $\sqrt{12} = \pm 5 \pmod{13}$.
Quadratic Residues

Example: If \( n = 21 \) (composite)

\[
\begin{array}{cccccccccccc}
  y: & 1 & 2 & 4 & 5 & 8 & 10 & 11 & 13 & 16 & 17 & 19 & 20 \\
\hline
  y^2: & 1 & 4 & 16 & 4 & 1 & 16 & 16 & 1 & 4 & 16 & 4 & 1 \\
\end{array}
\]

Thus, \( QR_{21} = \{1, 4, 16\} \), and 
\( QNR_{21} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\} \). Note that \( 3^3 = 9 \) (mod 21), or \( 7^2 = 7 \) (mod 21), but 3, 9, and 7 are not in \( \mathbb{Z}^*_{21} \). Each square root now has 4 solutions:

\[
\sqrt{1} = \pm 1 \pmod{21}, \quad \text{and} \quad \sqrt{1} = \pm 8 \pmod{21},
\]
\[
\sqrt{4} = \pm 2 \pmod{21}, \quad \text{and} \quad \sqrt{4} = \pm 5 \pmod{21},
\]
\[
\sqrt{16} = \pm 4 \pmod{21}, \quad \text{and} \quad \sqrt{16} = \pm 10 \pmod{21}.
\]
Legendre Symbol, Euler’s Criterion

Definition: Legendre symbol. Suppose $p$ is an odd prime. Then, for any $x$, the Legendre symbol $L(x, p)$ is defined as

$$L(x, p) = \begin{cases} 0, & \text{if } x \equiv 0 \pmod{p}, \\ 1, & \text{if } x \in \mathbb{QR}_p, \\ -1, & \text{if } x \in \mathbb{QNR}_p. \end{cases}$$

$L(x, p)$ can be computed easily using the following theorem.

Theorem: Euler’s criterion. For all primes $p > 2$, and all $x \in \mathbb{Z}_p$

$$x^{(p-1)/2} = L(x, p) \pmod{p}.$$
Euler’s Criterion

Proof: If $x = 0$ the result is trivially true. Thus, assume that $x \in \mathbb{Z}_p^*$. Then, according to Fermat’s Little Theorem, $x^{p-1} = 1 \pmod{p}$ and either

$$x^{(p-1)/2} = 1 \pmod{p}, \quad \text{or} \quad x^{(p-1)/2} = -1 \pmod{p}.$$ 

If $x \in QR_p$, i.e., $x = y^2 \pmod{p}$ for some $y \in \mathbb{Z}_p^*$, then

$$x^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = 1 \pmod{p}.$$ 

Conversely, if $x \in QNR_p$, then $x \neq y^2 \pmod{p}$ for $y \in \mathbb{Z}_p^*$ and thus $x^{(p-1)/2}$ must be congruent to $-1$ modulo $p$. QED
Jacobi Symbol

Definition: Jacobi symbol. Let $n$ be any positive odd integer with prime factorization

$$ n = p_1^{e_1} \cdot p_2^{e_2} \cdots \cdot p_k^{e_k}. $$

Then, for any $x$, the Jacobi symbol $J(x, n)$ is defined as

$$ J(x, n) = L(x, p_1)^{e_1} \cdot L(x, p_2)^{e_2} \cdots \cdot L(x, p_k)^{e_k}. $$

An important special case in cryptography is the case $n = p \cdot q$, where $p$ and $q$ are distinct odd primes. In this case

$$ J(x, n) = \begin{cases} 
0, & \Rightarrow \gcd(x, n) \neq 1, \\
-1, & \Rightarrow x \in QNR_n, \\
1, & \Rightarrow x \in QR_n \text{ or } x \in QNR_n.
\end{cases} $$

If $J(x, n) = L(x, p) L(x, q) = 1$, it is impossible to tell whether $x \in QR_n$ or not since both $1 \times 1$ and $(-1) \times (-1)$ are equal to one. In the first case $x \in QR_n$, in the second case $x \in QNR_n$. 
Jacobi Symbol

Theorem: Properties of Jacobi symbol. The Jacobi symbol satisfies the following properties which make it easy to compute $J(x, n)$, $n$ odd:

1. $J(x \pm n, n) = J(x, n)$,
2. $J(x \cdot y, n) = J(x, n) \cdot J(y, n)$,
3. $J(x, m \cdot n) = J(x, m) \cdot J(x, n)$,
4. $J(1, n) = 1$
5. $J(-1, n) = (-1)^{(n-1)/2} = \begin{cases} 1, & \text{if } n \equiv 1 \pmod{4}, \\ -1, & \text{if } n \equiv -1 \pmod{4}. \end{cases}$
6. $J(2, n) = (-1)^{(n^2-1)/8} = \begin{cases} 1, & \text{if } n \equiv \pm 1 \pmod{8}, \\ -1, & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases}$
7. If $x, n$ odd and $\gcd(x, n) = 1$
   
   $J(x, n) \cdot J(n, x) = (-1)^{(x-1)(n-1)/4}$, or equivalently,

   $J(x, n) = \begin{cases} -J(n, x), & \text{if } x \equiv n \equiv 3 \pmod{4}, \\ J(n, x), & \text{otherwise}. \end{cases}$
Primality Tests

- A 
  decision problem
  is a problem where a question is posed that can be answered by “yes” or “no”.

- A probabilistic algorithm is an algorithm that uses some form of randomness, e.g., random numbers, during its execution.

- **Definition:** A yes-biased Monte Carlo Algorithm is a probabilistic algorithm for a decision problem in which a “yes” answer is always correct, but a “no” answer may be incorrect, e.g., with probability \( \leq \epsilon \).

- **Example:** The Solovay-Strassen algorithm is a yes-biased Monte Carlo algorithm for composite integers \( n \) with \( \epsilon = 1/2 \). Thus, if the algorithm answers “yes” then \( n \) is composite for sure, but if it answers “no” then \( n \) may still be composite, with probability \( \leq 1/2 \).
Pseudo-Primes

**Example:** According to Fermat’s Little Theorem, every prime $n$ must satisfy $x^{n-1} = 1 \pmod{n}$ for $x \in \mathbb{Z}_n$. Thus, if for a given $n$ an $x$ is found such that this statement is not true, then it is known that $n$ is composite. But some composites may actually pass this test, which motivates the following definition.

**Definition:** If $n$ is an odd composite number and $x \in \mathbb{Z}_n^*$ is an integer such that

$$x^{n-1} = 1 \pmod{n},$$

holds, then $n$ is called a **pseudo-prime to the base** $x$. The graph on the next slide shows the fraction of $x$ for which $n \leq 2500$ is a pseudo-prime.
Definition: A **Carmichael number** is a composite integer $n$ such that

$$x^{n-1} = 1 \pmod{n},$$

holds for every $x \in \mathbb{Z}_n^*$. The first few Carmichael numbers are 561, 1105, 1729, 2465.
**Euler Pseudo-Primes**

► **Definition:** Let \( n \) be an odd integer and let \( J(x, n) \) denote the Jacobi symbol. If \( n \) is composite and \( x \in \mathbb{Z}_n^* \) satisfies (cf. Euler’s criterion)

\[
x^{(n-1)/2} \equiv J(x, n) \pmod{n},
\]

then \( n \) is called an **Euler pseudo-prime to the base** \( x \). The graph on the next slide shows the fraction of \( x \) for which \( n \leq 2500 \) is an Euler pseudo-prime.

► **Example:** The number \( n = 91 = 7 \times 13 \) is an Euler pseudo-prime to the base \( x = 9 \) since (quite obviously \( 9 \in \text{QR}_{91} \))

\[
9^2 = 81, \quad 9^3 = 9 \times (-10) = 1 \quad \Rightarrow \quad 9^{(91-1)/2} = (9^3)^{15} = 1 = J(9, 91).
\]

But 91 is not an Euler pseudo-prime to the base 4 since

\[
4^{(91-1)/2} = (4^6)^7 \times 4^3 = 64 \neq J(4, 91) = 1.
\]

Question: Are there any composite numbers \( n \) which are Euler pseudo-primes to every \( x \in \mathbb{Z}_n^* \)?
Theorem: If $n$ is an odd composite integer, then $n$ is an Euler pseudo-prime to the base $x$ for at most 50% of all $x$ such that $gcd(x, n) = 1$. Holds with equality for $n = 1729, 2465, \ldots$. 
Solovay-Strassen Primality Test

**Theorem: Solovay-Strassen 1977.** For any odd integer $n > 1$ the following statements are equivalent:

1. $n$ is prime.
2. $x^{(n-1)/2} = J(x, n) \pmod{n}$ holds for all $x \in \mathbb{Z}_n^*$.

**Solovay-Strassen Primality Test.** This is a probabilistic test which is based on the above theorem. Assume $n > 1$ is an odd integer. The steps for each test are:

1. Choose a random integer $x$, $1 < x < n - 1$.
2. If $J(x, n) = x^{(n-1)/2} \pmod{n}$ then answer “$n$ is prime,” else answer “$n$ is composite.”

**Note:** It will never happen that the answer is “$n$ is composite” if $n$ is indeed a prime. But with probability at most $1/2$ it can happen that the answer is “$n$ is prime” if $n$ is indeed composite. By repeating the test a sufficient number of times, the probability of error can be made arbitrarily small ($\approx 2^{-m}$ where $m$ is the number of tests performed).
Strong Pseudo-Primes

- **Theorem: Miller 1976.** For any odd integer $n > 1$ write $n - 1 = 2^s m$, where $m$ is odd. Then the following statements are equivalent:

  1. $n$ is prime.
  2. For all $x \in \mathbb{Z}_n^*$, if $x^m \not\equiv 1 \pmod{n}$, then there exists an $i$, $0 \leq i < k$ such that $x^{2^i m} = -1 \pmod{n}$.

- **Definition:** Let $n = 2^s m + 1$, $m$ odd, be an odd integer. If $n$ is composite and $x \in \mathbb{Z}_n^*$ satisfies

  either $x^m \equiv 1 \pmod{n}$,

  or there exists $i$, $0 \leq i < k$, such that $(x^m)^{2^i} = -1 \pmod{n}$,

  then $n$ is called a strong pseudo-prime to the base $x$. The graph on the next slide shows the fraction of $x$ for which $n \leq 2500$ is a strong pseudo-prime.
Example: Let \( n = 133 \) \((= 7 \times 19)\) and thus \( n - 1 = 132 = 2^2 \times 33 \). Testing with \( x \in \mathbb{Z}_{133}^* \) yields

\[
\begin{align*}
 x = 11 & : \quad 11^{33} = 1 \quad \implies \quad "n \text{ is prime}" \\
 x = 12 & : \quad 12^{33} = 132 \quad \implies \quad "n \text{ is prime}" \\
 x = 13 & : \quad 13^{33} = 27, \quad (13^{33})^2 = 64 \quad \implies \quad "n \text{ is composite}"
\end{align*}
\]

\( n = 133 \) is strong pseudo-prime to base 11, 12, but not to base 13.
Miller-Rabin Primality Test

Miller-Rabin Primality Test. This is a probabilistic test which is based on Miller’s theorem. Assume $n > 1$ is an odd integer and write $n - 1 = 2^s m$, where $m$ is odd. The steps for each test are:

1. Choose a random integer $x$, $1 < x < n - 1$.
2. Compute $b = x^m \pmod{n}$
3. If $b = 1 \pmod{n}$ then answer “$n$ is prime” and stop.
4. For $i = 0$ to $s - 1$ do
5. If $b = -1 \pmod{n}$ then answer “$n$ is prime” and stop, else $b \leftarrow b^2 \pmod{n}$
6. If you did not quit in step (3) or (5), answer “$n$ is composite.”

Note: Like in the Solovay-Strassen test, it will never happen in the Miller-Rabin test that the answer is “$n$ is composite” if $n$ is indeed a prime. But with probability at most $1/4$ it can happen that the answer is “$n$ is prime” if $n$ is indeed composite. By repeating the test a sufficient number of times, the probability of error can be made arbitrarily small ($\approx 4^{-m}$ where $m$ is the number of tests performed).