Mathematics for Cryptography

Dhananjoy Dey

Indian Institute of Information Technology, Lucknow
ddey@iiitl.ac.in

January 20, 2021

Disclaimers

1

All the pictures used in this presentation are taken from freely available websites.

Disclaimers

1

All the pictures used in this presentation are taken from freely available websites.

2

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

Outline

1. Maths for Symmetric/Private Key Crypto
   - Algebra
   - Rings
   - Finite Fields

2. Maths for Asymmetric/Public Key Crypto
   - Number Theory
     - Primality Testing

Outline

1. Maths for Symmetric/Private Key Crypto
   - Algebra
   - Rings
   - Finite Fields

2. Maths for Asymmetric/Public Key Crypto
   - Number Theory
     - Primality Testing

Group

Definition

1. *Let G be a non-empty set with a binary operation $\circ$ defined on it. Then $(G, \circ)$ is said to be a* ***groupoid*** *if $\circ$ is closed i.e. if $\circ : G \times G \longrightarrow G$.*
2. *A set G with an operation $\circ$ is said to be a* ***semigroup*** *if G is a groupoid and $\circ$ is associative.*
3. *A set G with an operation $\circ$ is said to be a* ***monoid*** *if G is a semigroup and $\exists$ an element $e \in G_m$ s/t $g.e = e.g = g \; \forall \; g \in G$.*
4. *For each $x \in G, \; \exists$ an element $y \in G$ s/t $y \circ x = x \circ y = e$. Usually, y is denoted by x^{-1}.*

If G satisfies all the above, it is said to be a ***Group****.*

If $x \circ y = y \circ x \; \forall \; x, y \in G$, G is called abelian or commutative group.

Example

1. $(\mathbb{Z}, +)$
2. $(\mathbb{Q}, +), (\mathbb{Q}, \cdot)$
3. $(\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$
4. $(\mathbb{Z}_n, +)$
5. $(\mathbb{Z}_p, \cdot)$

Group

- A group G is finite if $|G|$ or $\# G$ is finite. The number of elements in a finite group is called its ***order***.
- A non-empty subset H of a group G is a ***subgroup*** of G if H is itself a group w.r.t. the operation of G. If H is a subgroup of G and $H \neq G$, then H is called a proper subgroup of G.
- A group G is ***cyclic*** if $\exists\ \alpha \in G$ s/t for each $\beta \in G\ \exists$ integer i with $\beta = \alpha^i$. Such an element α is called a ***generator*** of G.
- Let $\alpha \in G$. The ***order*** of α is defined to be the least positive integer t s/t $\alpha^t = e$, provided that such an integer exists. If such a t does not exist, then the order of α is defined to be ∞.

Group

Theorem

Lagrange's Theorem: *If G is a finite group & H is a subgroup of G, then $\#H \mid \#G$.*
Hence, if $a \in G$, the order of a divides $\#G$.

- Every subgroup of a cyclic group is also cyclic.
  In fact, if G is a cyclic group of order n, then for each positive divisor d of n, G contains exactly one subgroup of order d.
- Let G be a group.
  - If the order of $a \in G$ is t, then the order of a^k is $\frac{t}{gcd(t, k)}$.
  - If G is a cyclic group of order n & $d \mid n$, then G has exactly $\phi(d)$ elements of order d. In particular, G has $\phi(n)$ generators.

Group

Example

1. *Consider the multiplicative group* $\mathbb{Z}_{19}^* = \{1, 2, \cdots, 18\}$ *of order 18.*

Subgroup	*Generators*	*Order*
$(\{1\}, \cdot)$	*1*	*1*
$(\{1, 18\}, \cdot)$	*18*	*2*
$(\{1, 7, 11\}, \cdot)$	*7, 11*	*3*
$(\{1, 7, 8, 11, 12, 18\}, \cdot)$	*8, 12*	*6*
$(\{1, 4, 5, 6, 7, 9, 11, 16, 17\}, \cdot)$	*4, 5, 6, 9, 16, 17*	*9*
$(\mathbb{Z}_{19}^*, \cdot)$	*2, 3, 10, 13, 14, 15*	*18*

2. *Consider the multiplicative group* $(\mathbb{Z}_{26}^*, \cdot)$

Definition

A ring $(R, +, \times)$ consists of a set R with 2 binary operations arbitrarily denoted by '$+$' & '$\times$' on R, satisfying the following conditions:

i. $(R, +)$ *is an abelian group with identity denoted* '0'.

ii. *The operation* $\times$ *is associative, i.e.,* $a \times (b \times c) = (a \times b) \times c \ \forall \ a, b, c \in R$.

iii. *The operation* $\times$ *is distributive over* $+$, *i.e.,*

- $a \times (b + c) = (a \times b) + (a \times c)$ &
- $(b + c) \times a = (b \times a) + (c \times a) \ \forall \ a, b, c \in R$.

Definition

A ring $(R, +, \times)$ consists of a set R with 2 binary operations arbitrarily denoted by '$+$' & '$\times$' on R, satisfying the following conditions:

i. $(R, +)$ *is an abelian group with identity denoted* '0'.
ii. *The operation* $\times$ *is associative, i.e.,* $a \times (b \times c) = (a \times b) \times c \ \forall \ a, b, c \in R$.
iii. *The operation* $\times$ *is distributive over* $+$, *i.e.,*
   - $a \times (b + c) = (a \times b) + (a \times c)$ &
   - $(b + c) \times a = (b \times a) + (c \times a) \ \forall \ a, b, c \in R$.

- The ring R is said to be **commutative ring** if $a \times b = b \times a \ \forall \ a, b \in R$.
- The ring R is said to be **ring with identity element** if $\exists \ 1$ s/t $a.1 = 1.a = a \ \forall \ a \in R$.

Example

1. $(2\mathbb{Z}, +, \cdot)$
2. $(\mathbb{Z}, +, \cdot)$
3. $(\mathbb{R}, +, \cdot)$
4. $(\mathbb{Z}_{26}, +, \cdot)$
5. *For a given value of* n*, the set of all* $n \times n$ *square matrices over* $\mathbb{R}$ *under the operations of matrix addition and matrix multiplication constitutes a ring.*

- If R is a commutative ring, then $a(\neq 0) \in R$ is said to be a **zero-divisor** it $\exists$ a $b \in R$ & $b \neq 0$ s/t $ab = 0$.

$$R = \mathbb{Z}_{26}; \qquad \text{2 \& 13 are } \textit{zero-divisors}$$

- A commutative ring R is said to be an **integral domain** if it has no *zero-divisors*.

$$R = \mathbb{Z} \ \ or \ \ \mathbb{R}$$

- A ring R is said to be a **division ring** if $(R \setminus \{0\}, \cdot)$ forms a group.

$$R = \mathbb{Z}_p$$

- A non-empty subset I of R is said to be a (2-sided) **ideal** of R if
  1. $(I, +) \leq (R, +)$
  2. $\forall\ u \in I\ \&\ r \in R,$ both $ur\ \&\ ru \in I$
- An ideal $M(\neq R)$ in a ring R is said to be **maximal ideal** of R if whenever I is an ideal of R s/t $M \subseteq I \subseteq R$ then either $R = I$ or $M = I$.
- An integral domain R with identity is a **principal ideal ring** if every ideal I in R is of the form $I =< \alpha >, \quad \alpha \in R$.

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An affine cipher is a simple substitution where

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$p_i \mapsto (a.p_i + b) \mod 26.$$

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An affine cipher is a simple substitution where

$$f_{a,b} : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$
$$p_i \mapsto (a.p_i + b) \mod 26.$$

Example

- *Encrypt* ***COLLEGE*** *using* $a = 5$ *and* $b = 4$

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An affine cipher is a simple substitution where

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$p_i \mapsto (a.p_i + b) \mod 26.$$

Example

- *Encrypt **COLLEGE** using $a = 5$ and $b = 4$*
- *Convert **C O L L E G E** in numeric form*

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An affine cipher is a simple substitution where

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$p_i \mapsto (a.p_i + b) \mod 26.$$

Example

- *Encrypt* ***COLLEGE*** *using* $a = 5$ *and* $b = 4$
- *Convert* ***C O L L E G E*** *in numeric form*

  2 14 11 11 4 6 4
- *Apply the affine function*

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An affine cipher is a simple substitution where

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$p_i \mapsto (a.p_i + b) \mod 26.$$

Example

- *Encrypt* ***COLLEGE*** *using* $a = 5$ *and* $b = 4$
- *Convert* ***C O L L E G E*** *in numeric form*

  2 14 11 11 4 6 4
- *Apply the affine function 14 22 7 7 24 8 24*
- *Cipher text is*

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An affine cipher is a simple substitution where

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$p_i \mapsto (a.p_i + b) \mod 26.$$

Example

- *Encrypt **COLLEGE** using $a = 5$ and $b = 4$*
- *Convert **C O L L E G E** in numeric form*

  2 14 11 11 4 6 4
- *Apply the affine function 14 22 7 7 24 8 24*
- *Cipher text is **OWHHYIY***

Ring $(\mathbb{Z}_{26}, +, \cdot)$ in Affine Cipher

- An affine cipher is a simple substitution where

$$f_{a,b} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \mapsto (a.x + b) \mod 26.$$

Exercise

1. *Let* $f_{(a,b)}$ & $f_{(c,d)}$ *be two affine ciphers s/t*

$$f_{(a,b)}(x) \equiv (a.x + b) \mod 26$$
$$f_{(c,d)}(x) \equiv (c.x + d) \mod 26$$

   Is $f_{(c,d)} \circ f_{(a,b)}$ *a stronger encryption scheme than* $f_{(a,b)}$*?*

2. *What is the key-space of an affine cipher?*

Ring $M_n(\mathbb{Z}_{26})$ in Hill Cipher – Poly-alphabetic Cipher

Hill Cipher[1]

- Encryption key,

$$K = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix}$$

[1] Hill cipher was developed by **Lester S. Hill**, an American mathematician.

Ring $M_n(\mathbb{Z}_{26})$ in Hill Cipher – Poly-alphabetic Cipher

Hill Cipher[1]

- Encryption key,

$$K = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix}$$

- The plaintext letters $p_1, p_2 \ \& \ p_3$ encrypted into ciphertext letters $c_1, c_2 \ \& \ c_3$ by

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

[1] Hill cipher was developed by **Lester S. Hill**, an American mathematician.

Ring $M_n(\mathbb{Z}_{26})$ in Hill Cipher – Poly-alphabetic Cipher

Example

$$Key = \begin{pmatrix} 10 & 1 & 14 \\ 11 & 9 & 4 \\ 5 & 22 & 9 \end{pmatrix}$$

Ring $M_n(\mathbb{Z}_{26})$ in Hill Cipher – Poly-alphabetic Cipher

Example

$$Key = \begin{pmatrix} 10 & 1 & 14 \\ 11 & 9 & 4 \\ 5 & 22 & 9 \end{pmatrix}$$

- *Encrypt the plaintext* ***ETE RNA LLI GHT***
- *The numerical form of the plaintext is* $4\ 19\ 4\quad 17\ 13\ 0\quad 11\ 11\ 8\quad 6\ 7\ 19$
- *The ciphertext is* *11 23 6 1 18 7 1 16 5 21 23 17*
  LXG BSH BQF VXR

Finite Fields

- A **finite field** is a field $\mathbb{F}$ which contains a finite number of elements.

Finite Fields

- A **finite field** is a field $\mathbb{F}$ which contains a finite number of elements.
- If $\mathbb{F}$ is a finite field, then $\mathbb{F}$ contains p^m elements for some prime p and integer $m \geq 1$.

Finite Fields

- A **finite field** is a field $\mathbb{F}$ which contains a finite number of elements.
- If $\mathbb{F}$ is a finite field, then $\mathbb{F}$ contains p^m elements for some prime p and integer $m \geq 1$.
- For every prime power order p^m, there is a $!$ finite field of order p^m. This field is denoted by $\mathbb{F}_{p^m}$, or sometimes by $GF(p^m)$.

Finite Fields

- A **finite field** is a field $\mathbb{F}$ which contains a finite number of elements.
- If $\mathbb{F}$ is a finite field, then $\mathbb{F}$ contains p^m elements for some prime p and integer $m \geq 1$.
- For every prime power order p^m, there is a $!$ finite field of order p^m. This field is denoted by $\mathbb{F}_{p^m}$, or sometimes by $GF(p^m)$.
- For $m = 1,\ \mathbb{F}_p$ or $GF(p)$ is a field. If p is a prime then $\mathbb{Z}_p$ is a field.

$$\mathbb{F}_p \cong GF(p) \cong \mathbb{Z}_p.$$

Finite Fields

- Let $\mathbb{F}_q$ be a finite field of order $q = p^m$.
  - Then every subfield of $\mathbb{F}_q$ has order p^n, for some n which is a positive divisor of m.
  - Conversely, if n is a positive divisor of m, then there is exactly one subfield of $\mathbb{F}_q$ of order p^n.

Finite Fields

- Let $\mathbb{F}_q$ be a finite field of order $q = p^m$.
  - Then every subfield of $\mathbb{F}_q$ has order p^n, for some n which is a positive divisor of m.
  - Conversely, if n is a positive divisor of m, then there is exactly one subfield of $\mathbb{F}_q$ of order p^n.
- The non-zero elements of $\mathbb{F}_q$ form a group under multiplication called the **multiplicative group** of $\mathbb{F}_q$, denoted by $\mathbb{F}_q^*$.

Finite Fields

- Let $\mathbb{F}_q$ be a finite field of order $q = p^m$.
  - Then every subfield of $\mathbb{F}_q$ has order p^n, for some n which is a positive divisor of m.
  - Conversely, if n is a positive divisor of m, then there is exactly one subfield of $\mathbb{F}_q$ of order p^n.
- The non-zero elements of $\mathbb{F}_q$ form a group under multiplication called the **multiplicative group** of $\mathbb{F}_q$, denoted by $\mathbb{F}_q^*$.
- $\mathbb{F}_q^*$ is a cyclic group of order $q-1$. Hence $a^q = a, \ \forall \ a \in \mathbb{F}_q$.

Finite Fields

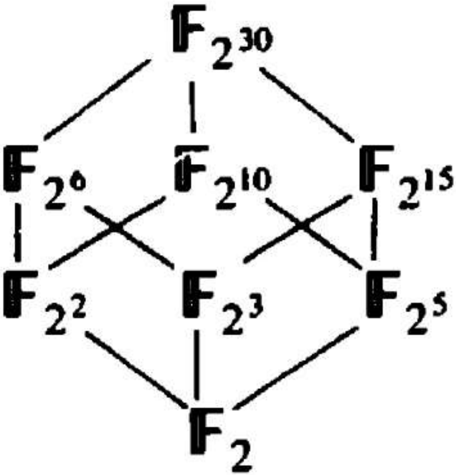
- Let $\mathbb{F}_q$ be a finite field of order $q = p^m$.
  - Then every subfield of $\mathbb{F}_q$ has order p^n, for some n which is a positive divisor of m.
  - Conversely, if n is a positive divisor of m, then there is exactly one subfield of $\mathbb{F}_q$ of order p^n.
- The non-zero elements of $\mathbb{F}_q$ form a group under multiplication called the **multiplicative group** of $\mathbb{F}_q$, denoted by $\mathbb{F}_q^*$.
- $\mathbb{F}_q^*$ is a cyclic group of order $q - 1$. Hence $a^q = a, \ \forall\ a \in \mathbb{F}_q$.
- A generator of the cyclic group $\mathbb{F}_q^*$ is called a **primitive element** or **generator** of $\mathbb{F}_q$.

Finite Fields

Subfields of $\mathbb{F}_{2^{30}}$ and their relation:

Finite Fields

Subfields of $\mathbb{F}_{2^{30}}$ and their relation:

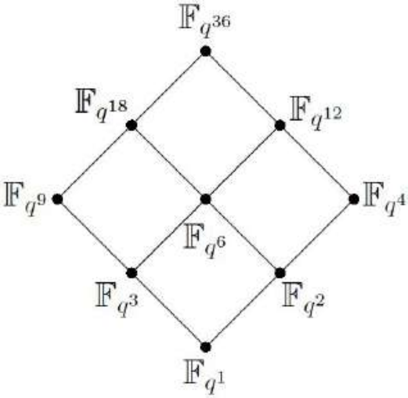


Finite Fields

Subfields of $\mathbb{F}_{q^{36}}$ and their relation:

Finite Fields

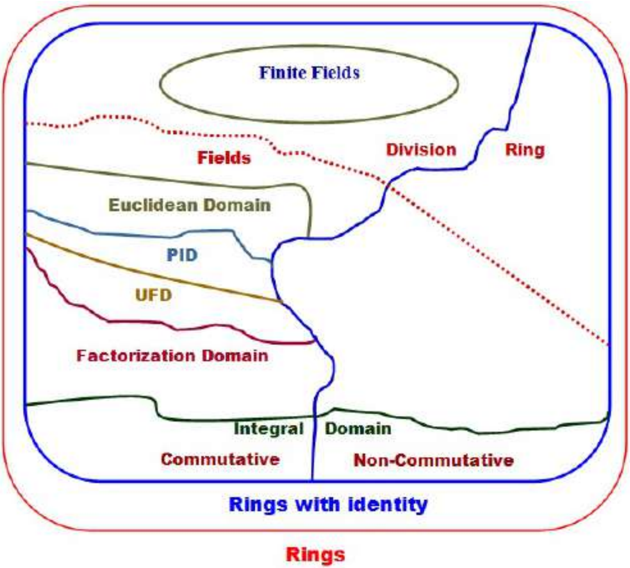
Subfields of $\mathbb{F}_{q^{36}}$ and their relation:



The subfields of $\mathbb{F}_{q^{36}}$

Types of Rings

Types of Rings



Construction of Finite Field of Order p^m

Construction of Finite Field of Order p^m

- First select an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m.
- The ideal $< f(x) >$ is

Construction of Finite Field of Order p^m

- First select an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m.
- The ideal $< f(x) >$ is a maximal ideal.
- Then $Z_p[x]/ < f(x) >$ is a

Construction of Finite Field of Order p^m

- First select an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m.
- The ideal $< f(x) >$ is a maximal ideal.
- Then $Z_p[x]/ < f(x) >$ is a finite field of order p^m.
- For each $m \geq 1$, $\exists$ a monic irreducible polynomial of degree m over $\mathbb{Z}_p$.

  Hence, every finite field has a polynomial basis representation.

Construction of Finite Field of Order p^m

Theorem

The number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n is given by

$$\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d},$$

where μ is Möbius function.

Construction of Finite Field of Order p^m

Theorem

The number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n is given by

$$\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d},$$

where μ is Möbius function.

Definition

TheMöbius function μ is the function on $\mathbb{N}$ defined by

$$\mu(n) = \begin{cases} 1 & if\ n = 1, \\ (-1)^k & if\ n\ is\ the\ product\ of\ k\ distinct\ primes, \\ 0 & if\ n\ is\ divisible\ by\ square\ of\ a\ prime. \end{cases}$$

Computing Multiplicative Inverses in $\mathbb{F}_{p^m}$

Algorithm

Input: a non-zero polynomial $g(x) \in \mathbb{F}_{p^m}$[a].

Output: $g(x)^{-1} \in \mathbb{F}_{p^m}$.

Computing Multiplicative Inverses in $\mathbb{F}_{p^m}$

Algorithm

Input: a non-zero polynomial $g(x) \in \mathbb{F}_{p^m}$[a].

Output: $g(x)^{-1} \in \mathbb{F}_{p^m}$.

1. Use the extended Euclidean algorithm for polynomials to find 2 polynomials $s(x)$ & $t(x) \in \mathbb{Z}_p[x]$ s/t

$$s(x)g(x) + t(x)f(x) = 1.$$

Computing Multiplicative Inverses in $\mathbb{F}_{p^m}$

Algorithm

Input: a non-zero polynomial $g(x) \in \mathbb{F}_{p^m}$[a].

Output: $g(x)^{-1} \in \mathbb{F}_{p^m}$.

1. Use the extended Euclidean algorithm for polynomials to find 2 polynomials $s(x)$ & $t(x) \in \mathbb{Z}_p[x]$ s/t

$$s(x)g(x) + t(x)f(x) = 1.$$

2. *Return*($s(x)$).

[a] The elements of the field $\mathbb{F}_{p^m}$ are represented as $\mathbb{Z}_p[x]/ < f(x) >$, where $f(x) \in \mathbb{Z}_p[x]$ is an irreducible polynomial of degree m over $\mathbb{Z}_p$.

Finite Fields

Definition

*An irreducible polynomial $f \in \mathbb{Z}_p[x]$ of degree m is called a **primitive polynomial** if α is a generator of $\mathbb{F}^*_{p^m}$, the multiplicative group of all the non-zero elements in $\mathbb{F}_{p^m} = \mathbb{Z}_p[x]/ < f(x) >$, where α is a root of the polynomial $f(x)$ over its extension field.*

Finite Fields

Definition

An irreducible polynomial $f \in \mathbb{Z}_p[x]$ of degree m is called a ***primitive polynomial*** *if α is a generator of $\mathbb{F}^*_{p^m}$, the multiplicative group of all the non-zero elements in $\mathbb{F}_{p^m} = \mathbb{Z}_p[x]/ < f(x) >$, where α is a root of the polynomial $f(x)$ over its extension field.*

- The irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m is a primitive polynomial iff $f(x) \mid x^k - 1$ for $k = p^m - 1$ and for no smaller positive integer k.

Finite Fields

Definition

An irreducible polynomial $f \in \mathbb{Z}_p[x]$ of degree m is called a ***primitive polynomial*** *if α is a generator of $\mathbb{F}^*_{p^m}$, the multiplicative group of all the non-zero elements in $\mathbb{F}_{p^m} = \mathbb{Z}_p[x]/ < f(x) >$, where α is a root of the polynomial $f(x)$ over its extension field.*

- The irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree m is a primitive polynomial iff $f(x) \mid x^k - 1$ for $k = p^m - 1$ and for no smaller positive integer k.
- For each $m \geq 1$, $\exists$ a monic primitive polynomial of degree m over $\mathbb{Z}_p$. In fact, there are precisely $\frac{\phi(p^m-1)}{m}$ such polynomials.

Example

- **Addition (in the field $GF(2^8)$)**
  The sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 of the coefficients of the two terms.

Example

- **Addition (in the field $GF(2^8)$)**
  The sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 of the coefficients of the two terms.

Example

$$57 + 83 = ?$$

Example

- **Addition (in the field $GF(2^8)$)**
  The sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 of the coefficients of the two terms.

Example

$$57 + 83 = ?$$

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2 = D4$$

Example

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8. For Rijndael, the inventors selected the following irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1 \; or \; 11B.$$

Example

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8. For Rijndael, the inventors selected the following irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1 \ or \ 11B.$$

Example

$$57 \times 83 = ?$$

Example

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8. For Rijndael, the inventors selected the following irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1 \; or \; 11B.$$

Example

$$57 \times 83 = ?$$

$$(x^6 + x^4 + x^2 + x + 1) \times (x^7 + x + 1)$$

$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

Example

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8. For Rijndael, the inventors selected the following irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1 \; or \; 11B.$$

Example

$$57 \times 83 = ?$$

$$(x^6 + x^4 + x^2 + x + 1) \times (x^7 + x + 1)$$
$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$
$$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \; mod \; m(x)$$
$$= x^7 + x^6 + 1 = C1$$

Outline

1. Maths for Symmetric/Private Key Crypto
   - Algebra
   - Rings
   - Finite Fields
2. Maths for Asymmetric/Public Key Crypto
   - Number Theory
     - Primality Testing

What is Number Theory?

Number theory is concerned mainly with the study of the properties (e.g., the divisibility) of the integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots, \},$$

particularly the positive integers $Z^+ = \{1, 2, 3, \ldots\}$.

What is Number Theory?

Number theory is concerned mainly with the study of the properties (e.g., the divisibility) of the integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots, \},$$

particularly the positive integers $Z^+ = \{1, 2, 3, \ldots\}$.

For example, in divisibility theory, all positive integers can be classified into three classes:

1. Unit: 1.
2. Prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, ...
3. Composite numbers: 4, 6, 8, 9, 10, 12, 14, 15, ...

Famous Quotations Related to Number Theory

The great mathematician **Carl Friedrich Gauss** called this subject *arithmetic* and he said:

"*Mathematics is the queen of sciences and arithmetic the queen of mathematics.*"

Famous Quotations Related to Number Theory

Prof G. H. Hardy

In the 1^{st} quotation Prof Hardy is speaking of the famous Indian Mathematician Ramanujan. This is the source of the often made statement that Ramanujan knew each integer personally.

1. I remember once going to see him when he was lying ill at Putney. I had ridden in taxi cab number 1729 and remarked that number seemed to me rather dull one and that I hoped it was not an unfavorable omen. “No", he replied it is a very interesting number; it is the smallest number expressible as the sum of cubes of two integers in two different ways.

Famous Quotations Related to Number Theory

Prof G. H. Hardy

In the 1^{st} quotation Prof Hardy is speaking of the famous Indian Mathematician Ramanujan. This is the source of the often made statement that Ramanujan knew each integer personally.

1. I remember once going to see him when he was lying ill at Putney. I had ridden in taxi cab number 1729 and remarked that number seemed to me rather dull one and that I hoped it was not an unfavorable omen. “No", he replied it is a very interesting number; it is the smallest number expressible as the sum of cubes of two integers in two different ways.
2. Pure mathematics is on the whole distinctly more useful than applied. For what is useful above all is technique and mathematical technique is taught mainly through pure mathematics.

The Floor & Ceiling of a Real Number

Definition

1. *The* ***floor*** *or the* ***greatest integer*** *function is defined as*

$$\lfloor x \rfloor \;=\; max\{n \in \mathbb{Z} \;:\; n \leq x\}$$

2. *The* ***ceiling*** *or the* ***least integer*** *function is defined as*

$$\lceil x \rceil \;=\; min\{n \in \mathbb{Z} \;:\; n \geq x\}$$

3. *The* ***nearest integer*** *function is defined as*

$$\lfloor x \rceil \;= \lfloor x + 1/2 \rfloor$$

Computational Number Theory

Computational Number Theory := Number Theory $\oplus$ Computation Theory

$\Downarrow$	$\Downarrow$	$\Downarrow$
Primality Testing	Elementary Number Theory	Computability Theory
Integer Factorization	Algebraic Number Theory	Complexity Theory
Discrete Logarithms	Combinatorial Number Theory	Infeasibility Theory
Elliptic Curves	Analytic Number Theory	Computer Algorithms
Conjecture Verification	Arithmetic Algebraic Geometry	Computer Architectures
Theorem Proving	Probabilistic Number Theory	Quantum Computing
	Applied Number Theory	Biological Computing
$\vdots$	$\vdots$	$\vdots$

Modular Arithmetic

- **The Division Algorithm:** If $a, b \in \mathbb{Z}$ & $b > 0$, then $\exists\,!\ q$ & $r \in \mathbb{Z}$ s/t

$$a = q.b + r, \ \ where\ 0 \leq r < b.$$

q is called the **quotient** and r is called the **remainder**.

Modular Arithmetic

- **The Division Algorithm:** If $a, b \in \mathbb{Z}$ & $b > 0$, then $\exists\, !\; q$ & $r \in \mathbb{Z}$ s/t

$$a = q.b + r, \; where \; 0 \le r < b.$$

  q is called the **quotient** and r is called the **remainder**.

- We can also write

$$a \;\equiv\; r \; mod \; b$$

Modular Arithmetic

- **The Division Algorithm:** If $a, b \in \mathbb{Z}$ & $b > 0$, then $\exists\, !\ q$ & $r \in \mathbb{Z}$ s/t

$$a = q.b + r,\ where\ 0 \leq r < b.$$

  q is called the **quotient** and r is called the **remainder**.

- We can also write

$$a \equiv r \ mod\ b$$

- Let $a, b \in \mathbb{Z}$. If $a \neq 0$ & $b \neq 0$, we define **greatest common divisor** or $gcd(a,\ b)$ to be the largest integer d s/t $d \mid a$ & $d \mid b$. We define $gcd(0, 0) = 0$.

Modular Arithmetic

Euclidean algorithm for computing the $gcd(a, b)$

Input: 2 non-negative integers a & b, $with\ a \geq b$.

Output: $gcd(a, b)$

1. While $(b \neq 0)$ do
   1.1 Set $r \leftarrow a \ mod\ b$, $a \leftarrow b,\ b \leftarrow r$.
2. *Return*(a)

Modular Arithmetic

Euclidean algorithm for computing the $gcd(a, b)$

Input: 2 non-negative integers a & b, $with\ a \geq b$.

Output: $gcd(a, b)$

1. While $(b \neq 0)$ do
   1.1 Set $r \leftarrow a \ mod \ b$, $a \leftarrow b, \ b \leftarrow r$.
2. *Return*(a)

$gcd(4864, 3458)$

Modular Arithmetic

Euclidean algorithm for computing the $gcd(a, b)$

Input: 2 non-negative integers a & b, with $a \geq b$.

Output: $gcd(a, b)$

1. While $(b \neq 0)$ do
   1.1 Set $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$.
2. *Return*(a)

$gcd(4864, 3458)$

$$
\begin{aligned}
4864 &= 1.3458 + 1406\\
3458 &= 2.1406 + 646\\
1406 &= 2.646 + 114\\
646 &= 5.114 + 76\\
114 &= 1.76 + 38\\
76 &= 2.38 + 0.
\end{aligned}
$$

Modular Arithmetic

Euclidean algorithm for computing the $gcd(a, b)$

Input: 2 non-negative integers a & b, $with\ a \geq b$.

Output: $gcd(a, b)$

1. While $(b \neq 0)$ do
   1.1 Set $r \leftarrow a \bmod b$, $a \leftarrow b,\ b \leftarrow r$.
2. *Return*(a)

$gcd(4864, 3458)$

$$\begin{aligned} 4864 &= 1.3458 + 1406 \\ 3458 &= 2.1406 + 646 \\ 1406 &= 2.646 + 114 \\ 646 &= 5.114 + 76 \\ 114 &= 1.76 + 38 \\ 76 &= 2.38 + 0. \end{aligned}$$

Bezout's Lemma

$\forall\ a, b \in \mathbb{Z},\ \exists\ s, t \in \mathbb{Z}$ s/t $gcd(a, b) = s.a + t.b$

Modular Arithmetic

Extended Euclidean algorithm

Input: 2 non-negative integers a & b, $with\ a \geq b$.
Output: $d = \ gcd(a, b)$ & $x, y \in \mathbb{Z}$ s/t $ax + by = d$.

1. If $b = 0$ then set $d \leftarrow a,\ x \leftarrow 1,\ y \leftarrow 0$, and $return(d, x, y)$.
2. Set $x_2 \leftarrow 1,\ x_1 \leftarrow 0,\ y_2 \leftarrow 0,\ y_1 \leftarrow 1$.
3. While $(b > 0)$ do
    - 3.1 $q \leftarrow \lfloor a/b \rfloor,\ r \leftarrow a - qb,\ x \leftarrow x_2 - qx_1,\ y \leftarrow y_2 - qy_1$.
    - 3.2 $a \leftarrow b,\ b \leftarrow r,\ x_2 \leftarrow x_1,\ x_1 \leftarrow x,\ y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4. Set $d \leftarrow a,\ x \leftarrow x_2,\ y \leftarrow y_2$, and $return(d, x, y)$.

Modular Arithmetic

Extended Euclidean algorithm

Input: 2 non-negative integers a & b, *with* $a \geq b$.
Output: $d = gcd(a, b)$ & $x, y \in \mathbb{Z}$ s/t $ax + by = d$.

1. If $b = 0$ then set $d \leftarrow a,\ x \leftarrow 1,\ y \leftarrow 0$, and $return(d, x, y)$.
2. Set $x_2 \leftarrow 1,\ x_1 \leftarrow 0,\ y_2 \leftarrow 0,\ y_1 \leftarrow 1$.
3. While $(b > 0)$ do
   - 3.1 $q \leftarrow \lfloor a/b \rfloor,\ r \leftarrow a - qb,\ x \leftarrow x_2 - qx_1,\ y \leftarrow y_2 - qy_1$.
   - 3.2 $a \leftarrow b,\ b \leftarrow r,\ x_2 \leftarrow x_1,\ x_1 \leftarrow x,\ y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4. Set $d \leftarrow a,\ x \leftarrow x_2,\ y \leftarrow y_2$, and $return(d, x, y)$.

$a = 4864,\ b = 3458$

Modular Arithmetic

Extended Euclidean algorithm

Input: 2 non-negative integers a & b, $with\ a \geq b$.
Output: $d = gcd(a, b)$ & $x, y \in \mathbb{Z}$ s/t $ax + by = d$.

1. If $b = 0$ then set $d \leftarrow a,\ x \leftarrow 1,\ y \leftarrow 0$, and $return(d, x, y)$.
2. Set $x_2 \leftarrow 1,\ x_1 \leftarrow 0,\ y_2 \leftarrow 0,\ y_1 \leftarrow 1$.
3. While $(b > 0)$ do
   - 3.1 $q \leftarrow \lfloor a/b \rfloor,\ r \leftarrow a - qb,\ x \leftarrow x_2 - qx_1,\ y \leftarrow y_2 - qy_1$.
   - 3.2 $a \leftarrow b,\ b \leftarrow r,\ x_2 \leftarrow x_1,\ x_1 \leftarrow x,\ y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4. Set $d \leftarrow a,\ x \leftarrow x_2,\ y \leftarrow y_2$, and $return(d, x, y)$.

$a = 4864,\ b = 3458$

q	r	x	y	a	b	x_2	x_1	y_2	y_1
–	–	–	–	4864	3458	1	0	0	1
1	1406	1	−1	3458	1406	0	1	1	−1
2	646	−2	3	1406	646	1	−2	−1	3
2	114	5	−7	646	114	−2	5	3	−7
5	76	−27	38	114	76	5	−27	−7	38
1	38	32	−45	76	38	−27	32	38	−45
2	0	−91	128	38	0	32	−91	−45	128

$38 = 32.4864 - 45.3458$

Modular Arithmetic

The set $\mathbb{Z}_n$ and its properties

- $\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$

Modular Arithmetic

The set $\mathbb{Z}_n$ and its properties

- $\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$
- Is $\mathbb{Z}_n$ a group? If so, what is the group operator?

Modular Arithmetic

The set $\mathbb{Z}_n$ and its properties

- $\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$
- Is $\mathbb{Z}_n$ a group? If so, what is the group operator?
- Is $\mathbb{Z}_n$ an abelian group?

Modular Arithmetic

The set $\mathbb{Z}_n$ and its properties

- $\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$
- Is $\mathbb{Z}_n$ a group? If so, what is the group operator?
- Is $\mathbb{Z}_n$ an abelian group?
- Is $\mathbb{Z}_n$ a ring?

Modular Arithmetic

The set $\mathbb{Z}_n$ and its properties

- $\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$
- Is $\mathbb{Z}_n$ a group? If so, what is the group operator?
- Is $\mathbb{Z}_n$ an abelian group?
- Is $\mathbb{Z}_n$ a ring?
- Why is $\mathbb{Z}_n$ not an integral domain?

Modular Arithmetic

The set $\mathbb{Z}_n$ and its properties

- $\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$
- Is $\mathbb{Z}_n$ a group? If so, what is the group operator?
- Is $\mathbb{Z}_n$ an abelian group?
- Is $\mathbb{Z}_n$ a ring?
- Why is $\mathbb{Z}_n$ not an integral domain?

Note that the multiplicative inverses exist for only those elements of $a \in \mathbb{Z}_n$ that are relatively prime to n, i.e., $gcd(a, n) = 1$

Modular Arithmetic

- The existence of the multiplicative inverse for an element $a \in \mathbb{Z}_n$ is predicated on a being relatively prime to n.

Modular Arithmetic

- The existence of the multiplicative inverse for an element $a \in \mathbb{Z}_n$ is predicated on a being relatively prime to n.
- 2 integers a & b are said to be **relatively prime** or **coprime** if $gcd(a,\ b) = 1$.

Modular Arithmetic

- The existence of the multiplicative inverse for an element $a \in \mathbb{Z}_n$ is predicated on a being relatively prime to n.
- 2 integers a & b are said to be **relatively prime** or **coprime** if $gcd(a,\ b) = 1$.
- An integer $p \geq 2$ is said to be **prime** if its only positive divisors are 1 & p. Otherwise, p is called **composite**.

Modular Arithmetic

- The existence of the multiplicative inverse for an element $a \in \mathbb{Z}_n$ is predicated on a being relatively prime to n.
- 2 integers a & b are said to be **relatively prime** or **coprime** if $gcd(a,\ b) = 1$.
- An integer $p \geq 2$ is said to be **prime** if its only positive divisors are 1 & p. Otherwise, p is called **composite**.
- There are an infinite number of prime numbers.
- If $n > 1$ is composite then n has a prime divisor $p \leq \sqrt{n}$

Prime Numbers

Prime Number Theorem

Let $\pi(x)$ denote the number of prime numbers $\leq x$. Then

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$$

Prime Numbers

Prime Number Theorem

Let $\pi(x)$ denote the number of prime numbers $\leq x$. Then

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$$

Fundamental Theorem of Arithmetic

Every integer $n \geq 2$ has a factorization as a product of prime powers:

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

where the p_i are distinct primes, and the e_i are positive integers. Furthermore, the factorization is ! up to rearrangement of factors.

Strong Prime Number

Definition

A prime p is called a strong prime if

1. (i) $p - 1$ *has a large prime factor, say* r,
2. (ii) $p + 1$ *has a large prime factor, and*
3. (iii) $r - 1$ *has a large prime factor.*

Definition

For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1,\ n]$ which are relatively prime to n. The function ϕ is called the ***Euler phi function****.*

Definition

For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1,\ n]$ which are relatively prime to n. The function ϕ is called the ***Euler phi function****.*

Properties of Euler phi function

i. If p is a prime, then $\phi(p) = p - 1$.

Definition

For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1, \ n]$ which are relatively prime to n. The function ϕ is called the ***Euler phi function****.*

Properties of Euler phi function

i. If p is a prime, then $\phi(p) = p - 1$.
ii. The Euler phi function is multiplicative. That is, if $gcd(m, n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n).$$

Definition

For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1,\ n]$ which are relatively prime to n. The function ϕ is called the ***Euler phi function****.*

Properties of Euler phi function

i. If p is a prime, then $\phi(p) = p - 1$.

ii. The Euler phi function is multiplicative. That is, if $gcd(m, n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n).$$

iii. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, is the prime factorization of n, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Modular Arithmetic

Chinese Remainder Theorem

If the integers $n_1, n_2, \cdots, n_k$ are pairwise relatively prime, then the system of simultaneous congruences

$$x \equiv a_i \; mod \; n_i,$$

for $1 \leq i \leq k$ has a ! solution modulo $n = n_1 n_2 \cdots n_k$ which is given by

$$x = \sum_{i=1}^{k} a_i N_i M_i \; mod \; n,$$

where $N_i = n/n_i \;\&\; M_i = N_i^{-1} \; mod \; n_i$.

Repeated Square Algorithm for Integers in $\mathbb{Z}_n$

Algorithm

Input: b, m, n
Output: $b^m \mod n$
$P \leftarrow 1$
if $m = 0$ **then**
    return P
end
while $m \neq 0$ **do**
    if m *is odd* **then**
        $P \leftarrow P.b \mod n$
    end
    $m \leftarrow \lfloor \frac{m}{2} \rfloor$
    $b \leftarrow b^2 \mod n$
end
Return: P

Modular Arithmetic

- The multiplicative group of $\mathbb{Z}_n$ is

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \ : \ gcd(a,n) = 1\}.$$

Modular Arithmetic

- The multiplicative group of $\mathbb{Z}_n$ is

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \ : \ gcd(a, n) = 1\}.$$

- **Fermat's theorem:** If $gcd(a, p) = 1$, then

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

Modular Arithmetic

- The multiplicative group of $\mathbb{Z}_n$ is

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \ : \ gcd(a, n) = 1\}.$$

- **Fermat's theorem:** If $gcd(a, p) = 1$, then

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

- **Euler's theorem:** If $a \in \mathbb{Z}_n^*$, then

$$a^{\phi(n)} \equiv 1 \ mod \ n.$$

Modular Arithmetic

Properties of generators of $\mathbb{Z}_n^*$

i. $\mathbb{Z}_n^*$ has a generator iff $n = 2, 4, p^k \ or \ 2p^k$, where p is an odd prime and $k \geq 1$.

Modular Arithmetic

Properties of generators of $\mathbb{Z}_n^*$

i. $\mathbb{Z}_n^*$ has a generator iff $n = 2, 4, p^k \; or \; 2p^k$, where p is an odd prime and $k \geq 1$.

ii. Suppose that α is a generator of $\mathbb{Z}_n^*$. Then $b = \alpha^i \; mod \; n$ is also a generator of $\mathbb{Z}_n^*$ iff $gcd(i, \phi(n)) = 1$. It follows that if $\mathbb{Z}_n^*$ is cyclic, then the number of generators is $\phi(\phi(n))$.

Modular Arithmetic

Properties of generators of $\mathbb{Z}_n^*$

i. $\mathbb{Z}_n^*$ has a generator iff $n = 2, 4, p^k \; or \; 2p^k$, where p is an odd prime and $k \geq 1$.

ii. Suppose that α is a generator of $\mathbb{Z}_n^*$. Then $b = \alpha^i \; mod \; n$ is also a generator of $\mathbb{Z}_n^*$ iff $gcd(i, \phi(n)) = 1$. It follows that if $\mathbb{Z}_n^*$ is cyclic, then the number of generators is $\phi(\phi(n))$.

iii. $\alpha \in \mathbb{Z}_n^*$ is a generator of $\mathbb{Z}_n^*$ iff $\alpha^{\phi(n)/p} \not\equiv 1 \; mod \; n$ for each prime divisor p of $\phi(n)$.

Probabilistic Algorithm

Definition

*A **probabilistic algorithm** is an algorithm that uses random numbers.*

*A probabilistic algorithm for a decision problem is called **yes-biased Monte Carlo** algorithm if the answer YES is always correct, but a NO answer may be incorrect.*

We say that the algorithm has error probability ϵ if the probability that the algorithm will answer NO when the answer is actually YES is ϵ.

Probabilistic Algorithm

Pseudo-prime Test

Input: n
Output: YES if n is composite, NO otherwise.
Choose a random $b, \ 0 < b < n$
if $\gcd(b, n) > 1$ **then**
  return YES
end
else
;
if $b^{n-1} \not\equiv 1 \mod n$ **then**
  return YES
end
else ;
return NO

Probabilistic Algorithm

Miller-Rabin Test

Input: an odd integer $n \geq 3$ and security parameter $t \geq 1$.
Output: an answer "prime" or "composite" to the question: "Is n prime?"
Write $n - 1 = 2^s.r$ s/t r is odd.

for $i = 1$ *to* t **do**
    Choose a random integer a s/t $2 \leq a \leq n - 2$.
    Compute $y \equiv a^r \mod n$
    if $y \neq 1$ & $y \neq n - 1$ **then**
        $j \leftarrow 1.$
        while $j \leq s - 1$ & $y \neq n - 1$ **do**
            Compute $y \leftarrow y^2 \mod n.$
            If $y = 1$ then **return**("composite").
            $j \leftarrow j + 1$.
        end
        If $y \neq n - 1$ then **return** ("composite").
    end
end

Return("prime").

Deterministic Polynomial Time Algorithm

The AKS Algorithm

Input: a positive integer $n > 1$

Output: n is **Prime** or **Composite** in deterministic polynomial-time

If $n = a^b$ with $a \in \mathbb{N}$ & $b > 1$, then output **COMPOSITE.**

Deterministic Polynomial Time Algorithm

The AKS Algorithm

Input: a positive integer $n > 1$

Output: n is **Prime** or **Composite** in deterministic polynomial-time

If $n = a^b$ with $a \in \mathbb{N}$ & $b > 1$, then output **COMPOSITE.**

Find the smallest r such that $ord_r(n) > 4(\log n)^2$.

If $1 < \gcd(a, n) < n$ for some $a \leq r$, then output **COMPOSITE**.

Deterministic Polynomial Time Algorithm

The AKS Algorithm

Input: a positive integer $n > 1$

Output: n is **Prime** or **Composite** in deterministic polynomial-time

If $n = a^b$ with $a \in \mathbb{N}$ & $b > 1$, then output **COMPOSITE.**

Find the smallest r such that $ord_r(n) > 4(\log n)^2$.

If $1 < \gcd(a, n) < n$ for some $a \leq r$, then output **COMPOSITE**.

If $n \leq r$, then output **PRIME**.

Deterministic Polynomial Time Algorithm

The AKS Algorithm

Input: a positive integer $n > 1$

Output: n is **Prime** or **Composite** in deterministic polynomial-time

If $n = a^b$ with $a \in \mathbb{N}$ & $b > 1$, then output **COMPOSITE.**

Find the smallest r such that $ord_r(n) > 4(\log n)^2$.

If $1 < \gcd(a, n) < n$ for some $a \leq r$, then output **COMPOSITE**.

If $n \leq r$, then output **PRIME.**

for $a = 1$ *to* $\lfloor 2\sqrt{\phi(r)}\log n \rfloor$ **do**

    if $(x - a)^n \not\equiv (x^n - a) \mod (x^r - 1, n)$,

    then output **COMPOSITE.**

end

Return("PRIME").

Primitive Root

Definition

The smallest positive integer e *s/t*

$$a^e \equiv 1 \mod m$$

is called exponent of a *modulo* m *and is denoted by*

$$e = exp_m(a).$$

If $exp_m(a) = \phi(m)$*, then* a *is called* ***primitive root*** $\mod m$.

Some Facts About Primitive Roots

- Primitive roots exist only for the following moduli:
  $m = 1, 2, 4, p^\alpha \ \& \ 2p^\alpha$, where p is an odd prime $\alpha \geq 1$.
- If a is a generator of $\mathbb{Z}_m^*$, then
  $\mathbb{Z}_m^* = \{a^i \mod m \ : \ 0 \leq i \leq \phi(m) - 1\}$
- Suppose that a is a generator of $\mathbb{Z}_m^*$. Then $b = a^i \mod m$ is also a generator of $\mathbb{Z}_m^*$ iff $\gcd(i, \phi(m)) = 1$. It follows that if $\mathbb{Z}_m^*$ is cyclic, then the number of generators is $\phi(\phi(m))$.
- a is a generator of $\mathbb{Z}_m^*$ iff $a^{\phi(m)/p} \not\equiv 1 \mod m$ for each prime divisor p of $\phi(m)$.

The End

Thanks a lot for your attention!