Mathematical Background

Chester Rebeiro

March 7, 2017

Modular Arithmetic

Division Theorem

- Let n be a positive integer
- Let a be any integer
- a/n leaves a quotient q and remainder r such that

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor$$

- a is congruent to b modulo m, if a/m leaves a remainder b
- we write this as $a \equiv b \mod m$

Division Theorem

- Let n be a positive integer
- Let a be any integer
- a/n leaves a quotient q and remainder r such that

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor$$

- a is congruent to b modulo m, if a/m leaves a remainder b
- we write this as $a \equiv b \mod m$
- Examples
  - $13 \equiv 3 \mod 5$

Division Theorem

- Let n be a positive integer
- Let a be any integer
- a/n leaves a quotient q and remainder r such that

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor$$

- a is congruent to b modulo m, if a/m leaves a remainder b
- we write this as $a \equiv b \mod m$
- Examples
  - $13 \equiv 3 \mod 5$
  - $7 \equiv 1 \mod 3$

Division Theorem

- Let n be a positive integer
- Let a be any integer
- a/n leaves a quotient q and remainder r such that

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor$$

- a is congruent to b modulo m, if a/m leaves a remainder b
- we write this as $a \equiv b \mod m$
- Examples
  - $13 \equiv 3 \mod 5$
  - $7 \equiv 1 \mod 3$
  - $23 \equiv -1 \mod 12$

Division Theorem

- Let n be a positive integer
- Let a be any integer
- a/n leaves a quotient q and remainder r such that

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor$$

- a is congruent to b modulo m, if a/m leaves a remainder b
- we write this as $a \equiv b \mod m$
- Examples
  - $13 \equiv 3 \mod 5$
  - $7 \equiv 1 \mod 3$
  - $23 \equiv -1 \mod 12$
  - $20 \equiv 0 \mod 10$

Division Theorem

- Let n be a positive integer
- Let a be any integer
- a/n leaves a quotient q and remainder r such that

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor$$

- a is congruent to b modulo m, if a/m leaves a remainder b
- we write this as $a \equiv b \mod m$
- Examples
  - $13 \equiv 3 \mod 5$
  - $7 \equiv 1 \mod 3$
  - $23 \equiv -1 \mod 12$
  - $20 \equiv 0 \mod 10$
- If $b = 0$, we say m divides a. This is denoted $m|a$

Equivalent Statements

All these statments are equivalent

- $a \equiv b \mod m$
- For some constant k, $a = b + km$
- $m|(a - b)$
- When divided by m, a and b leave the same remainder

Equivalence Relations

Congruence $\mod m$ is an equivalence relation on intergers

- Reflexivity : any integer is congruent to itself $\mod m$
- Symmetry : $a \equiv b(\mod m)$ implies that $b \equiv a(\mod m)$.
- Transitivity : $a \equiv b(\mod m)$ and $b \equiv a(\mod m)$ implies that $a \equiv c(\mod m)$

Residue Class

It consists of all integers that leave the same remainder when divided by m

- The residue classes $\mod 4$ are
  $[0]_4 = \{..., -16, -12, -8, -4, 0, 4, 8, 12, 16, ...\}$
  $[1]_4 = \{..., -15, -11, -7, -3, 1, 5, 9, 13, 17, ...\}$
  $[2]_4 = \{..., -14, -10, -6, -2, 2, 6, 10, 14, 18, ...\}$
  $[3]_4 = \{..., -13, -9, -5, -1, 3, 7, 11, 15, 19, ...\}$
- The complete residue class $\mod 4$ has one 'representative' from each set $[0]_4, [1]_4, [2]_4, [3]_4$. This is denoted Z/mZ.
  - Complete residue Classes for $\mod 4$: $\{0, 1, 2, 3\}$

Theorem

If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then

- $-a \equiv -b \pmod m$
- $a + c \equiv b + d \pmod m$
- $ac \equiv bd \pmod m$

Problems to Solve

- Prove that $2^{32} + 1$ is divisible by 641
- Prove that if the sum of all digits in a number is divisible by 9, then the number itself is divisible by 9.

GCD

- GCD of two integers is the largest positive integer that divides both numbers without a remainder
- Examples
  - $gcd(8, 12) = 4$
  - $gcd(24, 18) = 6$
  - $gcd(5, 8) = 1$
- If $gcd(a, b) = 1$ and $a \geq 1$ and $b \geq 2$, then a and b are said to be relatively prime

Euler-Toient Function

- $\phi(n)$
- Counts the number of integers less than or equal to n that are relatively prime to n
- $\phi(1) = 1$
- example : $\phi(9) = 6$

Euler-Toient Function

- $\phi(n)$
- Counts the number of integers less than or equal to n that are relatively prime to n
- $\phi(1) = 1$
- example : $\phi(9) = 6$ ... verify !!
- example2 : $\phi(26) = ?$

Euler-Toient Function

- $\phi(n)$
- Counts the number of integers less than or equal to n that are relatively prime to n
- $\phi(1) = 1$
- example : $\phi(9) = 6$ ...verify !!
- example2 : $\phi(26) =?$ ...12
- If p is prime, then $\phi(p) = p - 1$

Properties of ϕ

- If m and n are relatively prime then $\phi(m \times n) = \phi(m) \times \phi(n)$
  - $\phi(77) = \phi(7 \times 11) = 6 \times 10 = 60$
  - $\phi(1896) = \phi(3 \times 8 \times 79) = 2 \times 4 \times 78 = 624$

More Properties

If p is a prime number then,

- $\phi(p^a) = p^a - p^{a-1}$
  - Evident for $a = 1$
  - For $a > 1$, out of the elements 1, 2, $\cdots$ p^a, the elements p, $2p$, $3p$ $\cdots$ $p^{a-2}p$ are not coprime to p^a

More Properties

If p is a prime number then,

- $\phi(p^a) = p^a - p^{a-1}$
  - Evident for $a = 1$
  - For $a > 1$, out of the elements 1, 2, $\cdots$ p^a, the elements p, $2p$, $3p$ $\cdots$ $p^{a-2}p$ are not coprime to p^a
- $\phi(p^a) = p^a - p^{a-1} = p^a(1 - 1/p)$

contd..

- Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are primes then
- $\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_k^{a_k})$
  $= n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k)$

contd..

- Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are primes then
- $\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_k^{a_k})$
  $= n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k)$
- eg. Find $\phi(60)$?

Prove that...

For $n > 2$, prove that $\phi(n)$ is even.

Fermat's Little Theorem

- If $gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \mod m$
- Find the remainder when 72^{1001} is divided by 31
  - $72 \equiv 10 \mod 31$, therefore $72^{1001} \equiv 10^{1001} \mod 31$
  - Now from Fermat's Little Theorem, $10^{30} \equiv 1 \mod 31$
  - Raising both sides to the power of 33, $10^{990} \equiv 1 \mod 31$
  - Thus,

$$
\begin{aligned}
&10^{1001} = 10^{990}10^{8}10^{2}10 && \\
&= 1(10^2)^4 10^2 10 && \text{by Fermat's little theorem} \\
&= 1(7)^4 7 * 10 && \text{using } 7 \equiv 10^2 \mod 31 \\
&= 49^2.7.10 && \text{using } 7^4 = (7^2)^2 \\
&= (-13)^2.7.10 && \text{using } 49 \equiv -13 \mod 31 \\
&= (14).7.10 && \text{using } -13 = 14 \mod 31 \\
&= 98.10 = 5.10 = 19 \mod 31 &&
\end{aligned}
$$

Finite Fields

Évariste Galois
(October 25, 1811 - May 31, 1832)

Groups, Abelian Groups, and Monoids

- Consider a set S and a binary function $*$ that maps $S \times S \rightarrow S$ ie. for every $(a, b) \in S \times S$, $*((a, b)) \in S$. This is denoted as $a * b$.

Groups, Abelian Groups, and Monoids

- Consider a set S and a binary function $*$ that maps $S \times S \rightarrow S$ ie. for every $(a, b) \in S \times S$, $*((a, b)) \in S$. This is denoted as $a * b$.
- Now consider a subset H of S

Groups, Abelian Groups, and Monoids

- Consider a set S and a binary function $*$ that maps $S \times S \to S$ ie. for every $(a, b) \in S \times S$, $*((a, b)) \in S$. This is denoted as $a * b$.
- Now consider a subset H of S
- $\langle H, * \rangle$ forms a **group** if the following properties are satisfied:

Groups, Abelian Groups, and Monoids

- Consider a set S and a binary function $*$ that maps $S \times S \rightarrow S$ ie. for every $(a, b) \in S \times S$, $*((a, b)) \in S$. This is denoted as $a * b$.
- Now consider a subset H of S
- $\langle H, * \rangle$ forms a **group** if the following properties are satisfied:
  - **Closure :** If $a, b \in H$ then $a * b \in H$

Groups, Abelian Groups, and Monoids

- Consider a set S and a binary function $*$ that maps $S \times S \rightarrow S$ ie. for every $(a, b) \in S \times S$, $*((a, b)) \in S$. This is denoted as $a * b$.
- Now consider a subset H of S
- $\langle H, * \rangle$ forms a **group** if the following properties are satisfied:
  - **Closure :** If $a, b \in H$ then $a * b \in H$
  - **Associativity :** If $a, b, c \in H$, then $(a * b) * c = a * (b * c)$

Groups, Abelian Groups, and Monoids

- Consider a set S and a binary function $*$ that maps $S \times S \to S$ ie. for every $(a, b) \in S \times S$, $*((a, b)) \in S$. This is denoted as $a * b$.
- Now consider a subset H of S
- $\langle H, * \rangle$ forms a **group** if the following properties are satisfied:
  - **Closure :** If $a, b \in H$ then $a * b \in H$
  - **Associativity :** If $a, b, c \in H$, then $(a * b) * c = a * (b * c)$
  - **Identity :** There exists a unique element e such that for all $a \in H$, $a * e = e * a = a$

Groups, Abelian Groups, and Monoids

- Consider a set S and a binary function $*$ that maps $S \times S \rightarrow S$ ie. for every $(a, b) \in S \times S$, $*((a, b)) \in S$. This is denoted as $a * b$.
- Now consider a subset H of S
- $\langle H, * \rangle$ forms a **group** if the following properties are satisfied:
  - **Closure :** If $a, b \in H$ then $a * b \in H$
  - **Associativity :** If $a, b, c \in H$, then $(a * b) * c = a * (b * c)$
  - **Identity :** There exists a unique element e such that for all $a \in H$, $a * e = e * a = a$
  - **Inverse :** For each $a \in H$, there exists and $a^{-1} \in H$ such that $a * a^{-1} = e$

Groups, Abelian Groups, and Monoids

- Consider a set S and a binary function $*$ that maps $S \times S \to S$ ie. for every $(a, b) \in S \times S$, $*((a, b)) \in S$. This is denoted as $a * b$.
- Now consider a subset H of S
- $\langle H, * \rangle$ forms a **group** if the following properties are satisfied:
  - **Closure :** If $a, b \in H$ then $a * b \in H$
  - **Associativity :** If $a, b, c \in H$, then $(a * b) * c = a * (b * c)$
  - **Identity :** There exists a unique element e such that for all $a \in H$, $a * e = e * a = a$
  - **Inverse :** For each $a \in H$, there exists and $a^{-1} \in H$ such that $a * a^{-1} = e$
- $\langle H, * \rangle$ is an **abelian group** if for all $a, b \in H$, $a * b = b * a$

Examples

- $\langle \mathbb{C}, + \rangle$ forms a group $\mathbb{C} = \{u + iv : u, v \in \mathbb{R}\}$
  - Closure and Associativity is satisfied
  - identity element 0
  - inverse $-u + i(-v)$

Examples

- $\langle \mathbb{C}, + \rangle$ forms a group $\mathbb{C} = \{u + iv : u, v \in \mathbb{R}\}$
  - Closure and Associativity is satisfied
  - identity element 0
  - inverse $-u + i(-v)$
- $\langle \mathbb{C}^*, \cdot \rangle$ forms a group
  - Closure and Associativity is satisfied
  - Identity Element : 1
  - Inverse of $u + iv \in C^*$ is

$$\frac{u}{u^2 + v^2} + i\frac{-v}{u^2 + v^2}$$

Examples

- $\langle \mathbb{C}, + \rangle$ forms a group $\mathbb{C} = \{u + iv : u, v \in \mathbb{R}\}$
  - Closure and Associativity is satisfied
  - identity element 0
  - inverse $-u + i(-v)$
- $\langle \mathbb{C}^*, \cdot \rangle$ forms a group
  - Closure and Associativity is satisfied
  - Identity Element : 1
  - Inverse of $u + iv \in C^*$ is

$$\frac{u}{u^2 + v^2} + i \frac{-v}{u^2 + v^2}$$

  - Note that $\langle \mathbb{C}, \cdot \rangle$ does not form a group, as 0 has no inverse.

Rings

A **ring** is defined by $\langle R, +, \cdot \rangle$ with the following properties

- $\langle R, + \rangle$ is an abelian group

Rings

A **ring** is defined by $\langle R, +, \cdot \rangle$ with the following properties

- $\langle R, + \rangle$ is an abelian group
- $\langle R, \cdot \rangle$ satisfies closure and associativity

Rings

A **ring** is defined by $\langle R, +, \cdot \rangle$ with the following properties

- $\langle R, + \rangle$ is an abelian group
- $\langle R, \cdot \rangle$ satisfies closure and associativity
- Multiplication distributes over addition
  - $a \cdot (b + c) = a \cdot b + a \cdot c$

Fields

Definition

A **field** is a commutative ring with unity, in which every non-zero element has an inverse. The field is denoted by $\langle F, +, \cdot \rangle$

Fields

Definition

A **field** is a commutative ring with unity, in which every non-zero element has an inverse. The field is denoted by $\langle F, +, \cdot \rangle$

...in other words

A **field** is a set with two commutative operations ($+$ and $\cdot$), in which one can add, subtract, and multiply any two elements, divide any element by another non-zero element, and multiplication distributes over addition.

Fields

Definition

A **field** is a commutative ring with unity, in which every non-zero element has an inverse. The field is denoted by $\langle F, +, \cdot \rangle$

...in other words

A **field** is a set with two commutative operations ($+$ and $\cdot$), in which one can add, subtract, and multiply any two elements, divide any element by another non-zero element, and multiplication distributes over addition.

Example

Set of real numbers, with operations addition and multiplication.

Finite Field

A field in which the set is finite

Finite Fields

- A *finite field* is a field with finite number of elements.
- The number of elements in the set is called the *order* of the field.
- A field with order m exists iff m is a prime power.
  - *i.e.* $m = p^n$, for some n and prime p
  - p is the *characteristic* of the finite field

Prime and Galois Field

Every finite field is of size p^n for some prime p and $n \in \mathbb{N}$ and is denoted as $\mathbb{F}_q = \mathbb{F}_{p^n}$

Prime Field ($\mathbb{F}_p$)

The finite field obtained when $n = 1$, ie. $\mathbb{F}_q = \mathbb{F}_p$

Galois Field ($\mathbb{F}_{p^n}$)

The finite field obtained when $n > 1$.
This is also known as extension field

Prime Field $\mathbb{F}_7$

- Identities : Additive Identity is 0, Multiplicative Identity is 1
- Addition Table for mod 7

+	0	1	2	3	4	5	6
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

(a) Addition modulo 7

- Multiplication Table for mod 7

×	0	1	2	3	4	5	6
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

(b) Multiplication modulo 7

Another Prime Field in $\mathbb{F}_2$

- Identity for addition is 0 and multiplication is 1
- Addition is by $\oplus$
- Multiplicaiton is by $\cdot$

Binary Fields

Binary fields are extension fields of the form $\mathbb{F}_2^m$. These fields have efficient representations in computers and are extensively used in cryptography.

How to construct an Extension Field

Constructing Galios Field $\mathbb{F}_{2^4}$ from $\mathbb{F}_2$.

1. Pick an irreducible polynomial $(f(x))$ of degree n with coefficients in $\mathbb{F}_2 = \{0, 1\}$

$$x^4 + x + 1$$

How to construct an Extension Field

Constructing Galios Field $\mathbb{F}_{2^4}$ from $\mathbb{F}_2$.

1. Pick an irreducible polynomial $(f(x))$ of degree n with coefficients in $\mathbb{F}_2 = \{0, 1\}$

$$x^4 + x + 1$$

2. Let θ be a root of $f(x)$.

$$f(\theta) : \theta^4 + \theta + 1 = 0$$

How to construct an Extension Field

Constructing Galios Field $\mathbb{F}_{2^4}$ from $\mathbb{F}_2$.

1. Pick an irreducible polynomial $(f(x))$ of degree n with coefficients in $\mathbb{F}_2 = \{0, 1\}$

$$x^4 + x + 1$$

2. Let θ be a root of $f(x)$.

$$f(\theta) : \theta^4 + \theta + 1 = 0$$

3. Given this equation, all other powers can be derived:

$$\theta^4 = \theta + 1$$
$$\theta^5 = \theta^4 \cdot \theta$$
$$\theta^6 = \theta^5 \cdot \theta^2$$
$$\cdots\cdots$$

closure is satisfied

How to construct an Extension Field

Constructing Galios Field $\mathbb{F}_{2^4}$ from $\mathbb{F}_2$.

1. Pick an irreducible polynomial $(f(x))$ of degree n with coefficients in $\mathbb{F}_2 = \{0, 1\}$

$$x^4 + x + 1$$

2. Let θ be a root of $f(x)$.

$$f(\theta) : \theta^4 + \theta + 1 = 0$$

3. Given this equation, all other powers can be derived:

$$\theta^4 = \theta + 1$$
$$\theta^5 = \theta^4 \cdot \theta$$
$$\theta^6 = \theta^5 \cdot \theta^2$$
$$\cdots\cdots$$

closure is satisfied

4. Therefore, it is sufficient that $\mathbb{F}_{2^4}$ contain all polynomials of degree $< n$.

-

Example : Consider the binary finite field $GF(2^4)$. there are 16 polynomials in the field.
The irreducible polynomial is $\theta^4 + \theta + 1$.

0	θ^2	θ^3	$\theta^3 + \theta^2$
1	$\theta^2 + 1$	$\theta^3 + 1$	$\theta^3 + \theta^2 + 1$
θ	$\theta^2 + \theta$	$\theta^3 + \theta$	$\theta^3 + \theta^2 + \theta$
$\theta + 1$	$\theta^2 + \theta + 1$	$\theta^3 + \theta + 1$	$\theta^3 + \theta^2 + \theta + 1$

Representation on a computer $\theta^3 + \theta + 1 \rightarrow (1011)_2$ ⋮Efficient !!!

Binary Field Arithmetic

Addition

Addition done by simple *XOR* operation.

$$(x^3 + x^2 + 1) + (x^2 + x + 1) = x^3 + x$$

Binary Field Arithmetic

Addition

Addition done by simple *XOR* operation.

$$(x^3 + x^2 + 1) + (x^2 + x + 1) = x^3 + x$$

Subtraction

Subtraction same as addition.

$$(\theta^3 + \theta^2 + 1) - (\theta^2 + x + 1) = \theta^3 + \theta$$

Binary Field Multiplication

$$
\begin{array}{cccccc}
 & & x^3 & +x^2 & +1 & \\
 & & x^2 & +x & +1 & \\
\hline
 & & x^3 & +x^2 & & +1 \\
 & x^4 & +x^3 & & +x & \\
x^5 & +x^4 & & +x^2 & & \\
\hline
x^5 & & & & +x & +1
\end{array}
$$

Binary Field Multiplication

$$
\begin{array}{cccccc}
 & & x^3 & +x^2 & +1 & \\
 & & x^2 & +x & +1 & \\
\hline
 & & x^3 & +x^2 & & +1 \\
 & x^4 & +x^3 & & +x & \\
x^5 & +x^4 & & +x^2 & & \\
\hline
x^5 & & & & +x & +1
\end{array}
$$

- $x^5 + x + 1$ is not in $GF(2^4)$

Binary Field Multiplication

$$
\begin{array}{cccccc}
 & & x^3 & +x^2 & +1 & \\
 & & x^2 & +x & +1 & \\
\hline
 & & x^3 & +x^2 & & +1 \\
 & x^4 & +x^3 & & +x & \\
x^5 & +x^4 & & +x^2 & & \\
\hline
x^5 & & & & +x & +1
\end{array}
$$

- $x^5 + x + 1$ is not in $GF(2^4)$
- Modular reduction $x^5 + x + 1 \, mod(x^4 + x + 1) = x^2 + 1$

Binary Field Multiplication

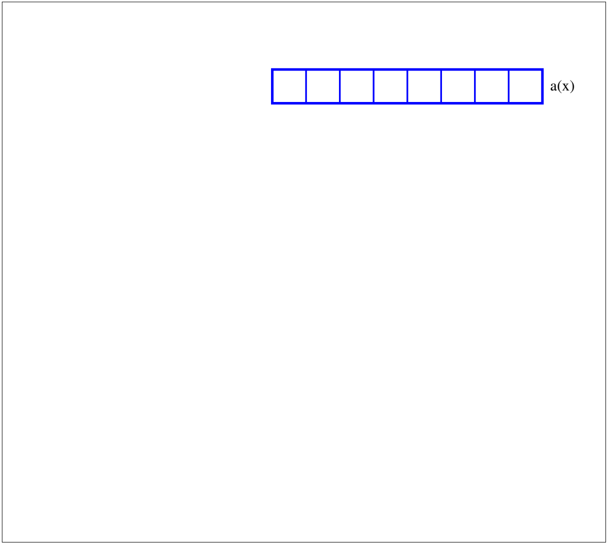
$$
\begin{array}{cccccc}
 & & x^3 & +x^2 & +1 & \\
 & & x^2 & +x & +1 & \\
\hline
 & & x^3 & +x^2 & & +1 \\
 & x^4 & +x^3 & & +x & \\
x^5 & +x^4 & & +x^2 & & \\
\hline
x^5 & & & & +x & +1
\end{array}
$$

- $x^5 + x + 1$ is not in $GF(2^4)$
- Modular reduction $x^5 + x + 1 \, mod(x^4 + x + 1) = x^2 + 1$

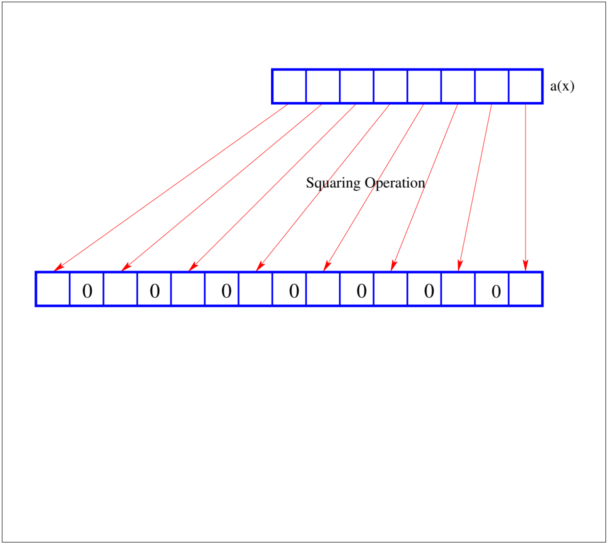
Efficient Multiplications

Karatsuba Multiplier, Mastrovito multiplier, Sunar-Koc multiplier, Massey-Omura multiplier, Montgomery multiplier

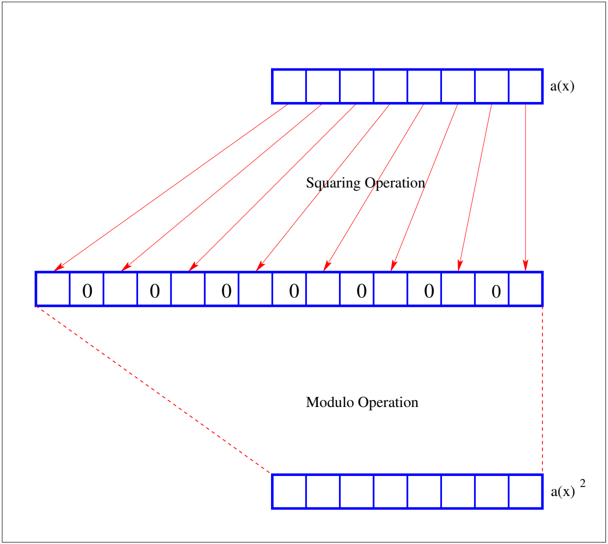
Squaring



Squaring



Squaring



Inversion

- Itoh-Tsujii Algorithm : Uses Fermat's Little Theorem
  - $\alpha^{2^m-1} = 1$
  - Thus, $\alpha\alpha^{2^m-2} = 1$
  - The inverse of α is α^{2^m-2}

Inversion

Determine the inverse of $a \in GF(2^{19})$ using Itoh-Tsujii Algorithm.

1. $a^{-1} = a^{2^{19}-2}$
2. Thus $a^{-1} = a^{2^{19}-1)^2}$
3. Take $\beta_k(a) = a^{2^k-1}$ ... therefore $a^{-1} = \beta_k(a)^2$
4. Consider the addition chain for $18 = (1,2,4,8,9,18)$
5. Consider the recursion $\beta_{m+n}(a) = \beta_m(a)^{2^n} \beta_n(a)$
6. Start from $\beta_1(a) = a$ and iterate the addition chain

Finite Fields and their Irreducible Polynomials

- Consider the fields in $GF(2^4)$. The elements in the field are

0	x^2	x^3	$x^3 + x^2$
1	$x^2 + 1$	$x^3 + 1$	$x^3 + x^2 + 1$
x	$x^2 + x$	$x^3 + x$	$x^3 + x^2 + x$
$x + 1$	$x^2 + x + 1$	$x^3 + x + 1$	$x^3 + x^2 + x + 1$

- Three irreducible polynomials of degree 4 that can generate the fields are:
  - $f_1(x) = x^4 + x + 1$ results in field $F1$
  - $f_2(x) = x^4 + x^3 + 1$ results in field $F2$
  - $f_3(x) = x^4 + x^3 + x^2 + x + 1$ results in field $F3$
- Note,
  - Each irreducible polynomial generates a different field with the same 16 elements
  - However operations within each field is different
    - $x \cdot x^4$ is $x + 1$ in $F1$
    - $x \cdot x^4$ is $x^3 + 1$ in $F2$
    - $x \cdot x^4$ is $x^3 + x^2 + x + 1$ in $F3$

Group Isomorphisms

- Given two groups $(G, \circ)$ and $(H, \bullet)$
- A *group isomorphism* is a bijective mapping $f : G \rightarrow H$ such that for all $u, v \in G$,

$$f(u \circ v) = f(u) \bullet f(v)$$

- If such a function f exists, G and H are said to be isomorphic.
- All finite fields of same order (number of elements) are **isomorphic**.

Isomorphic Field Mappings in $GF(2^4)$

- Consider isomorphic fields
  - $F_1 : GF(2^4)/(x^4 + x + 1)$ call this IR f_1
  - $F_2 : GF(2^4)/(x^4 + x^3 + 1)$ call this IR f_2
- To construct a mapping $T : F_1 \to F_2$ find $c \in F_2$ such that $f_1(c) \equiv 0 \mod (f_2)$.
  - This creates a mapping from $x \to c$
- For example : take $c = x^2 + x \in F_2$.
  - $f_1(c) = ((x^2 + x)^4 + (x^2 + x) + 1) mod f_2 \equiv 0$
  - This creates a map $T : x \to c$
  - Example:
    - Take $e_1 = x^2 + x$ and $e_2 = x^3 + x$
    - Verify $T(e_1 \times e_2 \mod f_1) = T(e_1) \times T(e_2) \mod f_2$

Composite Fields

1. Let $k = n \times m$, then $GF(2^n)^m$ is a composite field of $GF(2^k)$
2. For example,
   - $GF(2^4)^2$ is a composite fields of $GF(2^8)$
   - Elements in $GF(2^4)^2$ have the form $A_1x + A_0$ where a_1 and $a_0 \in GF(2^4)$
3. The composite field $GF(2^n)^m$ is isomorphic to $GF(2^k)$
   - Therefore we can define a map $f : GF(2^k) \rightarrow GF(2^n)^m$
   - and peform operations in the finite field
   - Typically operations such as inverse are easier done in composite fields

More Number Theory

The Multiplicative Inverse of an Element

- An element b in the ring $\mathbb{Z}_n$ has a multiplicative inverse iff $gcd(b, n) = 1$
- Finding $b^{-1} \mod n$:
  - using Extended Euclidan Algorithm

Euclidean Algorithm

Euclidean Algorithm to find GCD of a and b

Input: (a, b)
Output: $gcd(a, b)$

$r_0 \leftarrow a;$
$r_1 \leftarrow b;$
$m \leftarrow 1;$
while $r_m \neq 0$ **do**
    find q_m and r_{m+1} such that $r_{m-1} = r_m q_m + r_{m+1};$
    $m \leftarrow m + 1;$
end
return $r_{m-1} = gcd(a, b);$

Euclidean Algorithm (Example)

Find $gcd(62, 45)$

	$r_0 \leftarrow 62$	
	$r_1 \leftarrow 45$	
$62 = 45 \cdot 1 + 17$	$r_2 \leftarrow 17$	$q_1 \leftarrow 1$
$45 = 17 \cdot 2 + 11$	$r_3 \leftarrow 11$	$q_2 \leftarrow 2$
$17 = 11 \cdot 1 + 6$	$r_4 \leftarrow 6$	$q_3 \leftarrow 1$
$11 = 6 \cdot 1 + 5$	$r_5 \leftarrow 5$	$q_4 \leftarrow 1$
$6 = 5 \cdot 1 + 1$	$r_6 \leftarrow 1$	$q_5 \leftarrow 1$
$1 = 1 \cdot 1 + 0$	$r_7 \leftarrow 0$	$q_6 \leftarrow 1$

$gcd(62, 45) = r_6 = 1$

Euclidean Algorithm Working

Let $g = gcd(a, b)$, $r_0 \leftarrow a$, $r_1 \leftarrow b$

- Since $r_0 = q_1 r_1 + r_2$, $g|r_0$ and $g|r_1$, we have $g|r_2$.
- Further, g is the highest positive integer that divides both r_1 and r_2 (i.e. $g = gcd(r_1, r_2)$).
  - If this were not the case, then let $g' = gcd(r_1, r_2)$ and $g' > g$.
  - By the same argument as above, it can easily be shown that $g'|r_0$, thus $g' = gcd(r_0, r_1)$, implies $g = g'$.
- Thus, $g = gcd(r_0, r_1) = gcd(r_1, r_2) = gcd(r_2, r_3) = \cdots = gcd(r_{m-1}, r_m) = r_{m-1}$ since $r_m = 0$

Expressing r_i ($i \geq 2$) as linear combination of a and b

	$a = r_0 \leftarrow 62$ $b = r_1 \leftarrow 45$		
$62 = 45 \cdot 1 + 17$	$r_2 \leftarrow 17$	$q_1 \leftarrow 1$	$r_2 = r_0 - q_1 \cdot r_1$
$45 = 17 \cdot 2 + 11$	$r_3 \leftarrow 11$	$q_2 \leftarrow 2$	$r_3 = r_1 - q_2 \cdot r_2$ $= r_1 - q_2(r_0 - q_1 \cdot r_1)$ $= (1 - q_2 q_1) \cdot r_1 - q_2 r_0$
$17 = 11 \cdot 1 + 6$	$r_4 \leftarrow 6$	$q_3 \leftarrow 1$	$r_4 = r_2 - q_3 \cdot r_3$
$11 = 6 \cdot 1 + 5$	$r_5 \leftarrow 5$	$q_4 \leftarrow 1$	$r_5 = r_3 - q_4 \cdot r_4$
$6 = 5 \cdot 1 + 1$	$r_6 \leftarrow 1$	$q_5 \leftarrow 1$	$r_6 = r_4 - q_5 \cdot r_5$
$1 = 1 \cdot 1 + 0$	$r_7 \leftarrow 0$	$q_6 \leftarrow 1$	

$$\begin{aligned}
r_6 = 1 &= (1)6 - (1)5 \\
&= (1)6 - (1)(11 - (1)6) = (2)6 - 11 \\
&= (2)(17 - (1)11) - 11 = (2)17 - (3)11 \\
&= (2)17 - (3)(45 - (2)17) = (8)17 - (3)45 \\
&= (8)(62 - (1)45) - (3)45 \\
&= (8)62 - (11)45
\end{aligned}$$

Finding the inverse

If $gcd(a, b) = 1$, then

- $1 = x \cdot b + y \cdot a$
- Taking $\mod a$ on both sides
  - $1 \equiv x \cdot b \mod a$
  - Thus, the inverse of $b \mod a$ is x
- In our example, $a = 62$, $b = 45$, and $1 = (8)62 + (-11)45$
  - $1 \equiv (-11)45 \mod 62$
  - Thus the inverse of $45 \mod 62$ is $-11 \mod 62$, which is 51

Recurrences

$$t_j = \begin{cases} 0 & \text{if } j = 0 \\ 1 & \text{if } j = 1 \\ t_{j-2} - q_{j-1}t_{j-1} & \text{if } j \geq 2 \end{cases} \qquad s_j = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{if } j = 1 \\ s_{j-2} - q_{j-1}s_{j-1} & \text{if } j \geq 2. \end{cases}$$

For $0 \leq j \leq m$, we have that $r_j = s_j a + t_j b$

	$a = r_0 \leftarrow 62$ $b = r_1 \leftarrow 45$	
$62 = 45 \cdot 1 + 17$	$r_2 \leftarrow 17$	$q_1 \leftarrow 1$
$45 = 17 \cdot 2 + 11$	$r_3 \leftarrow 11$	$q_2 \leftarrow 2$
$17 = 11 \cdot 1 + 6$	$r_4 \leftarrow 6$	$q_3 \leftarrow 1$
$11 = 6 \cdot 1 + 5$	$r_5 \leftarrow 5$	$q_4 \leftarrow 1$
$6 = 5 \cdot 1 + 1$	$r_6 \leftarrow 1$	$q_5 \leftarrow 1$
$1 = 1 \cdot 1 + 0$	$r_7 \leftarrow 0$	$q_6 \leftarrow 1$

i	r_i	q_i	s_i	t_i	
0	62	-	1	0	
1	45	1	0	1	
2	17	2	1	-1	$17 = 1 \cdot 62 - 1 \cdot 45$
3	11	1	-2	3	$11 = -2 \cdot 62 + 3 \cdot 45$
4	6	1	3	-4	$6 = 3 \cdot 62 - 4 \cdot 45$
5	5	1	-5	7	$5 = -5 \cdot 62 + 7 \cdot 45$
6	1	1	8	11	$1 = 8 \cdot 62 - 11 \cdot 45$

Extended Euclidean Algorithm

Algorithm : EXTENDED EUCLIDEAN ALGORITHM(a, b)

$a_0 \leftarrow a$
$b_0 \leftarrow b$
$t_0 \leftarrow 0$
$t \leftarrow 1$
$s_0 \leftarrow 1$
$s \leftarrow 0$
$q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$
$r \leftarrow a_0 - qb_0$
while $r > 0$

do
$$\begin{cases} temp \leftarrow t_0 - qt \\ t_0 \leftarrow t \\ t \leftarrow temp \\ temp \leftarrow s_0 - qs \\ s_0 \leftarrow s \\ s \leftarrow temp \\ a_0 \leftarrow b_0 \\ b_0 \leftarrow r \\ q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor \\ r \leftarrow a_0 - qb_0 \end{cases}$$

$r \leftarrow b_0$
return (r, s, t)
comment: $r = \gcd(a, b)$ and $sa + tb = r$

A Small Improvement

If finding the inverse is the goal, then we could take mod 62 in each step.
We would not need the s_i recurrence in this case.

i	r_i	q_i	t_i	
0	62	-	0	
1	45	1	1	
2	17	2	-1	$17 \equiv -1 \cdot 45 \mod 62$
3	11	1	3	$11 \equiv 3 \cdot 45 \mod 62$
4	6	1	-4	$6 \equiv -4 \cdot 45 \mod 62$
5	5	1	7	$5 \equiv 7 \cdot 45 \mod 62$
6	1	1	11	$1 \equiv -11 \cdot 45 \mod 62$

Chinese Remainder Theorem (CRT)

Theorem.
Let m_1, m_2, $\cdots$, m_r be pairwise coprime. Let $M = m_1 \times m_2 \times m_3 \times \cdots \times m_r$. Then, $f(x) (\mod M) \equiv 0$ if $f(x) (\mod m_i) \equiv 0$ for $1 \leq i \leq r$.

Proof.
$M | f(x) \rightarrow f(x) = Mk$ for some constant k.
Thus, $f(x) = km_1 m_2 m_3 \cdots m_r \rightarrow m_i | f(x)$
for any i

Chinese Remainder Theorem

Chinese Remainder Theorem

Let $m_1, m_2, \cdots, m_r$ be pairwise coprime and $M = m_1 \times m_2 \times m_3 \times \cdots \times m_r$. Then the following system of congruences has a unique solution $\mod M$.

$$x \equiv a_i (\mod m_i) \qquad (1 \leq i \leq r)$$

Proof

- Let $M_i = M/m_i$ and $y_i \equiv M_i^{-1} (\mod m_i)$ for $1 \leq i \leq r$
- Note that $gcd(M_i, m_i) = 1$ for $1 \leq i \leq r$. Therefore the inverse y_i exists.
- Now notice, that $M_i y_i \equiv 1 (\mod m_i)$, therefore $a_i M_i y_i \equiv a_i (\mod m_i)$
- On the other hand, $M_i | m_j$ for $i \neq j$, thus $a_i M_i y_i \equiv 0 (\mod m_j)$.
- Thus $x \equiv \sum_{i=1}^{r} a_i M_i y_i (\mod m_j) \equiv a_j (\mod m_j)$

CRT Example

Find x

$$x \equiv 2 \pmod 3$$
$$x \equiv 2 \pmod 4,$$
$$x \equiv 1 \pmod 5$$

- Let : $m_1 = 3$, $m_2 = 4$, and $m_3 = 5$. $M = 3 \cdot 4 \cdot 5 = 60$
- Let : $M_1 = \frac{60}{3} = 20$ $\quad y_1 = 20^{-1} \pmod 3 = 2$
- $M_2 = \frac{60}{4} = 15$ $\quad y_2 = 15^{-1} \pmod 4 = 3$
- $M_3 = \frac{60}{5} = 12$ $\quad y_3 = 12^{-1} \pmod 5 = 3$

$$x = ((2 \cdot 20 \cdot 2) + (2 \cdot 15 \cdot 3) + (1 \cdot 12 \cdot 3)) \mod 60$$
$$= 206 \mod 60 \equiv 26$$