Introduction

- of increasing importance in cryptography
  - AES, Elliptic Curve, IDEA, Public Key
- concern operations on “numbers”
  - where what constitutes a “number” and the type of operations varies considerably
- start with concepts of **groups, rings, fields** from abstract algebra

A Group G

- A set of elements and some generic operation/s, with some certain **relations**:
- **Axioms:**
  - **A1 (Closure)** If $\{a,b\} \in G$, $\text{operated}(a,b) \in G$
  - **A2 (Associative)** law: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - **A3 (has identity) e**: $e \cdot a = a \cdot e = a$
  - **A4 (has inverses) a′**: $a \cdot a' = e$
- A G is a **finite group** if has a finite number of elements
- A G is **abelian** if it is commutative,
  - **A5 (has commutative)** $a \cdot b = b \cdot a$, for example;
  - The set of positive, negative, 0, integers under addition, identity is 0, inverse element is '–', inverse a = -a, a-b= a+(-b)
  - The set of nonzero real numbers under multiplication, identity is I, inverse element is division

- Suppose S_n is to be the set of permutations of n distinct symbols: {1,2,...,n}. S_n is a group!!:
- Suppose $\pi, \rho \in S_n$; **permutation operation π, and a group of S_n is ρ**; $\pi, \rho \in S_n$
  - **A1** $\pi_1 \cdot \rho = \pi_1 \cdot \{1,3,2\} = \{3,2,1\} \cdot \{1,3,2\} = \{2,3,1\} \in S_n$
  - *Change operator to arithmetic operators*..
  - **A2** $\pi_2 \cdot (\pi_1 \cdot \rho) = \{3,1,2\} \cdot \{2,3,1\} = \{3,1,2\}$

    $\therefore = (\pi_2 \cdot \pi_1) \cdot \rho = \{3,1,2\} \cdot \{3,2,1\} \cdot \{1,3,2\} = \{3,1,2\}$
  - **A3** identity $\{1, 2, 3, .., n\} \in S_n$
  - **A4** inverse that undoes π_1 is {3,2,1}, recovering earlier positions.

    $\{1,2,3\} \cdot \{2,3,1\} = \{2,3,1\}$, $\pi_1 \cdot \pi_1 = \{3,2,1\} \cdot \{3,2,1\} = \{1,2,3\}$
  - **A5** commutative!!.. $\{3,2,1\} \cdot \{2,3,1\} \neq \{2,3,1\} \cdot \{3,2,1\}$, so S_n is a group but not abelian

Cyclic Group

- A G is cyclic if every element $b \in G$ is a power of some fixed element a
  - ie $b = a^k$
- a is said to be a generator of the group G
  - example: $a^3 = a.a.a$ and identity be: $e = a^0 = 1$, and $a^{-n} = (a')^n \rightarrow a^n\ a^{-n} = 1$;
- The additive group of integers is an infinite cyclic group generated by the element 1. In this case, powers are interpreted additively, so that n is the n^th power of 1.

- A Ring *R* is an abelian group with two operations (addition and multiplication), satisfies **A1** to **A5**
  - A1-A5: for additiveness, identity is 0 and inverse is $-a$
  - M1: Closure under multiplication: if $a, b \in R$, then $ab \in R$.
  - M2: Associativity of multiplication: $a(bc) = (ab)c \in R$ for all $a, b, c \in R$.
  - M3: Distributive: $a(b+c)=ab+ac$, $(a+b)c=ac+bc$
  - WITHOUT LEAVING THE SET
- **M4: commutative ring** if $ba=ab$ for all $a, b, ab \in R$,
- **M5:** Multiplicative identity: $1a=a1=a$ for all $a, 1, ab \in R$
- **M6:** No zero divisors: If a and $b \in R$ and ab = 0, then either a = 0 or b = 0.

An **integral domain** is the one satisfies all the A1-5 and M1-6, which is then a commutative ring???, and abelian gr, and obeying M5-6. Cyclic??!!!

Field

- a set of numbers with two operations:
  - abelian group for addition: commutative for addition
  - abelian group for multiplication (ignoring 0): commutative for multiplication
  - It is a ring
- (A1-5, M1-6), F is an integral domain.
- **M7:** Multiplicative inverse. For each $a \in F$, except 0, there is an element $a^{-1} \in F$ such that $aa^{-1} = (a^{-1})a = 1$

Field

Integral domain

Commutative ring

Ring

Abelian group

Group

(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and a 0, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Modular Operations

- **Clock,** uses a **finite number** of values, and loops back from either end
- Associative, Distributive, Commutative,
- Identities: (0 + w)%n = w%n, (1·w)%n = w%n
- additive inv (-w)
- If `a=mb` (`a,b,m` all integers), `b|a`, `b` is divisor (*)
- Any **group** of integers: $Z_n = \{0, 1, \ldots, n-1\}$
- Form a **commutative ring** for **addition**
- with a multiplicative identity
- note **some peculiarities**
  - if `(a+b)≡(a+c)%(n)` then `b≡c%(n)`
  - but `(ab)≡(ac)%(n)` for all a,b,c $\in Z_n$
    then `b≡ c%(n)` only if `a` is relatively prime to `n`

%8 Example

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

Multiplication and inverses

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

Additive and multiplicative inverses modulo 8

a%(7), residue classes

[0]	[1]	[2]	[3]	[4]	[5]	[6]
−21	−20	−19	−18	−17	−16	−15
−14	−13	−12	−11	−10	−9	−8
−7	−6	−5	−4	−3	−2	−1
0	**1**	**2**	**3**	**4**	**5**	**6**
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34

. . .

Table 4.2. Properties of Modular Arithmetic for Integers in Z_n

- Commutative laws $(w + x) \bmod n = (x + w) \bmod n$
  $(w \times x) \bmod n = (x \times w) \bmod n$
- Associative laws

  $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$
  $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
- Distributive laws

  $[w + (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
  $[w + (x \times y)] \bmod n = [(w + x) \times (w + y)] \bmod n$
- Identities

  $(0 + w) \bmod n = w \bmod n$
  $(1 + w) \bmod n = w \bmod n$
- Additive inverse (-w)

  For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Relatively prime, Euclid's GCD Algorithm

- Numbers with gcd(a,b)=1 are relatively prime
  - eg GCD(8,15) = 1
- an efficient way to find the GCD(a,b), uses theorem that:

```
gcd(a,b) = gcd(b, a % b), (*)
```

- **Euclid's Algorithm** to compute GCD(a,b):

```
gcd(A, B)
1. While(B>0){
   1. r ← A % B;
   2. A ← B;
   3. B ← r;}
2. return A
```

Question is it possible to execute these in one line?

$\text{floor}(r_{i-2} / r_{i-1}) = r_i$

Multiplicative inverse (w^{-1})

- For a given prime, p, the finite field of order p, GF(p) is defined as the set Z_p of integers {0, 1,..., p - 1}, together with the arithmetic operations modulo p.
- For each $w \in Z_p$, $w \neq 0$, there exists a $w \in Z_p$, such that $w \times z \equiv 1 \pmod{p}$.
- Because w is relatively prime to p, if we multiply all the elements of Z_p by w, the resulting residues are all of the elements of Z_p permuted. Thus, exactly one of the residues has the value 1.

Galois Fields

- Galois fields are for polynomial eqns (group thry, number theory, Euclidian geometry): Algebraic solution to a polynomial eqn is related to the structure of a group of permutations associated with the roots of the polynomial, and an equation could be solvable in radicals if one can find a series of normal subgroups of its Galois group which are abelian, or its Galois group is solvable. (wikipedia)

- **Maths et histoire, evariste-galois.asp.htm**

- The finite field of order p^n is written GF(p^n).

- A field Z_n = {0,1,...,n-1} is **a commutative ring** in which every nonzero element is assumed to have a multiplicative inverse. 'a' is multiplicative inverse to n, iff integer is *relatively prime* to n.

- Definition: If n is a prime p, then GF(*p*) is defined as the set of integers Z_p={0, 1,..., *p*-1}, + operations in mod(*p*), then we can say the set Z_n of integers {0,1,...,n-1}, + operations in mod(n), is a commutative ring. "Well-behaving": the results of operations obtained are confined in the field of GF(p)
-
- We are interested in two finite fields of p^n, where *p* is prime,
  - GF(*p*)
  - GF(2^n)

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

w	$-w$	w^{-1}
0	0	—
1	1	1

The simplest finite field is GF(2).

×	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

GF(7)

(b) Multiplication modulo 7

Finding the Multiplicative Inverse in GF(p)

```
EXTENDED EUCLID(m, b)
1.   [A1,A2,A3; B1,B2,B3]←[1,0,m;0,1,b];
2. if B3==0;
        return(A3=gcd(m,b));      //no inverse
3. if B3==1;
        return(B3=gcd(m,b));
        B2=b^-1%m;
4. Q = ⌊A3/B3⌋;
5. [r1,r2,r3]←[A1−QB1, A2−QB2, A3−QB3];
6. [A1,A2,A3]←[B1,B2,B3];
7. [B1,B2,B3]←[r1,r2,r3];
8. goto 2
```

If (m, b) are relatively prime, then gcd(m, b) = 1, then b has a multiplicative inverse modulo m.

Inverse of 550 in GF(1759)

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	–3	109
5	1	–3	109	–5	16	5
21	–5	16	5	106	–339	4
1	106	–339	4	–111	355	1

Following the algorithm. Starting with step 0. Denote the **quotient** at step i by q_i.
Carry out each step of the Euclidean algorithm.
After the 2^{nd} step, calculate $p_i = p_{i-2} – p_{i-1}\, q_{i-2}$ %(n); p_0 =0, p_1 =1,
Continue to calculate for p_i one step more beyond the last step of the Euclidean algorithm.
If the last nonzero remainder occurs at step *k*, then if this remainder is 1, x has an inverse and it is p_{k+2}.
(If the remainder is not 1, then x does not have an inverse.)..

(21, 26) $p_i = p_{i-2} – p_{i-1}\, q_{i-2}$ %(m);
26 =1(21)+5; q_0 =1; p_0 = 0;
21 =4(5) +1; q_1 =4; p_1 = 1;
5 =5(1) +0; q_2 =5; p_2 = 0 -1(1)%(26) =-1%26=25.
p_3 = 1 -25(4)%(26) =1-22%26=25.
=-21%26=5.

(5, 26)
26 = 5(5)+1; q_0=5; p_0 =0;
5 = 5(1)+0; q_1=5; p_1 =1;
$p_2 = p_{i-2} – p_{i-1}\, q_{i-2}$ %(m) = 0-1(5)mod(26)=21;

****

Inverse of 550 in GF(1759)

$p_i = p_{i-2} – p_{i-1}\, q_{i-2}$ %(m);
1759 = 3(550)+109; q_0 = 3; p_0 = 0;
550 = 5(109)+5; q_1 = 5; p_1 = 1;
109 = 21(5)+4; q_2 = 21; p_2 = 0 - 1 (3) %(550) = -3.
5 = 1(4)+1; q_3 = 1; p_3 = 1 -(-3) (5) %(550) = 16
4 = 4(1)+0; q_4 = 4; p_4 =-3 - 16(21) %(550) = -339
p_5= 16 - -339 (1)%(550) = 355

Ordinary Polynomial

$$
\begin{array}{r}
x^3 + x^2 \phantom{{}-x} + 2 \\
+ \; (x^2 - x + 1) \\
\hline
x^3 + 2x^2 - x + 3
\end{array}
$$

(a) Addition

$$
\begin{array}{r}
x^3 + x^2 \phantom{{}-x} + 2 \\
- \; (x^2 - x + 1) \\
\hline
x^3 \phantom{{}+x^2} + x + 1
\end{array}
$$

(b) Subtraction

$$
\begin{array}{r}
x^3 + x^2 \phantom{{}-2x} + 2 \\
\times \; (x^2 - x + 1) \\
\hline
x^3 + x^2 \phantom{{}-2x} + 2 \\
- x^4 - x^3 \phantom{{}+x^2} - 2x \phantom{{}+2} \\
x^5 + x^4 \phantom{{}+x^3} + 2x^2 \phantom{{}-2x+2} \\
\hline
x^5 \phantom{{}+x^4+x^3} + 3x^2 - 2x + 2
\end{array}
$$

(c) Multiplication

$$
\begin{array}{r|l}
 & \phantom{x^3 + {}} x + 2 \\
\cline{2-2}
x^2 - x + 1 & x^3 + x^2 \phantom{{}-2x} + 2 \\
 & x^3 - x^2 + x \\
\cline{2-2}
 & \phantom{x^3 + {}} 2x^2 - x + 2 \\
 & \phantom{x^3 + {}} 2x^2 - 2x + 2 \\
\cline{2-2}
 & \phantom{x^3 + 2x^2 - 2x + {}} x
\end{array}
$$

(d) Division

Polynomial Arithmetic in Z_p

- Polynomial in which the coefficients are elements of some field *F,* is referred as *a polynomial over the field F*.
- Such polynomials set is referred to as a **polynomial ring**.

- Division is possible if the polynomial operations are performed *on polynomials over a field*, but exact division might not be possible. Tricky?..!!
- Within a field, two elements a and b, the quotient a/b is also an element of the field. However, given a ring R that is not a field, division will result in a quotient and a remainder; this is not exact division.
- 5, 3 within a set S. If S is the set of rational numbers, which is a field, then the result is simply expressed as 5/3 and is an element of S???. Suppose that S is the field $\mathbf{Z_7}$. **p=7**. In this case, $5/3 = (5 \times 3^{-1}) \bmod 7 = (5 \times 5) \bmod 7 = 4$ which is an **exact solution**. Suppose that S is the set of integers, which is a ring but not a field. Then 5/3 produces a quotient and a remainder: $5/3 = 1 + 2/3$; $5 = 1 \times 3 + 2$, division is not exact over the set of integers.

- **Division is not always defined, if it is over a coefficient set that is not a field**.

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

$$f(x) = q(x)g(x) + r(x)$$

Polynomial Arithmetic in Z_p if $r(x) = 0$, $g(x)|f(x)$, $g(x)$ is divisor.

- If the coefficient set is the integers, then $(5x^2)/(3x)$ does not have a solution, since not in the coefficient set.
- Suppose it is performed over Z_7. Then $(5x^2)/(3x) = 4x$ which is a valid polynomial over Z_7.
- Suppose, degree of f(x) is n, and of g(x) is m, n ≥ m, then degree of the quotient q(x), is (m-n) and of remainder is at most (m–1). Polynomial division is possible if the coefficient set is a field.
  - $r(x) = f(x) \bmod g(x)$
- $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$
- $q(x)g(x) + r(x) = (x + 2)(x^2 - x + 1) + x = (x^3 + x^2 - x + 2) + x = x^3 + x^2 + 2 = f(x)$
- Not convenient for logical operations such as XOR.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

w	$-w$	w^{-1}
0	0	—
1	1	1

The simplest finite field is GF(2).

×	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

GF(7)

(b) Multiplication modulo 7

		000	001	010	011	100	101	110	111
	+	0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

(a) Addition

6	7
8	4
7	7

GF(2^3)

		000	001	010	011	100	101	110	111
	×	0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

(b) Multiplication

w	$-w$	w^{-1}
0	0	—
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

(c) Additive and multiplicative inverses

In GF(2), **addition** and **multiplication** are equivalent to the **XOR**, and the logical **AND**, respectively. Addition and subtraction are equivalent. Therefore GF(2^n) is of most interest in.

$$
\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
+\,(x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4
\end{array}
$$

(a) Addition

$$
\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
-\,(x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4
\end{array}
$$

(b) Subtraction

$$
\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
\times\,(x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4 + x^3 + x + 1 \\
x^8 + x^6 + x^5 + x^4 + x^2 + x \\
x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 \\
\hline
x^{10} + x^4 + x^2 + 1
\end{array}
$$

(c) Multiplication

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\hline
x^3 + x + 1 & x^7 + x^5 + x^4 + x^3 + x + 1 \\
 & x^7 + x^5 + x^4 \\
\hline
 & x^3 + x + 1 \\
 & x^3 + x + 1 \\
\hline
\end{array}
$$

(d) Division

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n-1} a_i x^i$$

- Consider the set S of all polynomials of degree n-1 or less over the field Z_p. Thus, each polynomial has the form
- where each a_i takes on a value in the set {0, 1,..., p -1}. There are a total of p^n different polynomials in S.
- For p = 3 and n = 2, the $3^2 = 9$ polynomials in the set are
- 0 x 2x
- 1 x + 1 2x + 1
- 2 x + 2 2x + 2
- For p = 2 and n = 3, the $2^3 = 8$ the polynomials in the set are
- 0 x + 1 $x^2 + x$
- 1 x^2 $x^2 + x + 1$
- X $x^2 + 1$

- mod 2:
- $1 + 1 = 1 - 1 = 0$;
- $1 + 0 = 1 - 0 = 1$;
- $0 + 1 = 0 - 1 = 1$.

- if $f(x)$ has no divisors other than itself & 1 it is said **irreducible** (or prime) polynomial, an irreducible polynomial forms a field.
- $f(x) = x^4 + 1$ over GF(2) is reducible,
  - because $x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1)$
- $f(x) = x^3 + x + 1$ is irreducible residual 1.

$$
\begin{array}{r}
x^2 + x \phantom{{}+x+1} \\
x + 1 \,\big)\, \overline{x^3 \phantom{{}+x^2} + x + 1} \\
\underline{x^3 + x^2} \phantom{{}+x+1} \\
x^2 + x \phantom{{}+1} \\
\underline{x^2 + x} \phantom{{}+1} \\
1
\end{array}
$$

- eg. let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$
  $f(x) + g(x) = x^3 + x + 1$
- $f(x) \times g(x) = x^5 + x^2$

Finite Fields Of the Form $GF(2^n)$

- Polynomials over p^n, with $n > 1$, operations modulo p^n do not produce a field. There are structures satisfies the axioms for a field in a set with p^n elements, and concentrate on $GF(2^n)$.
- **Motivation** Virtually all encryption algorithms, both symmetric and public key, involve arithmetic operations on integers with divisions.
- For efficiency: integers that fit exactly into a given number of bits, with no wasted bit patterns, integers in the range 0 through 2^(n)-1, fitting into an n-bit word. Z_{256} versus Z_{251}

Polynomial GCD

- gcd[a(x), b(x)] is the polynomial of maximum degree that divides both a(x) and b(x).
- gcd[a(x), b(x)] = gcd[b(x), a(x)mod(b(x))]
- Euclid[$a(x)$, $b(x)$]
  1. $A(x) \Leftarrow a(x)$; $B(x) \Leftarrow b(x)$
  2. **if** $B(x) = 0$ **return** $A(x) = \gcd[a(x), b(x)]$
  3. $R(x) = A(x) \bmod B(x)$
  4. $A(x) \Leftarrow B(x)$
  5. $B(x) \Leftarrow R(x)$
  6. **goto** 2

Example of GCD in Z_2 or in GF(2),

Step1, gcd(A(x), B(x))

$A(x) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$,

$B(x) = x^4 + x^2 + x + 1$; $D(x)= x^2 + x$;

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

Step 2,

$A(x) = B(x) = x^4 + x^2 + x + 1$;

$B(x) = R(x) = x^3 + x^2 + 1$,

$D(x) = x + 1$; $R(x) =0$;

Step 3,

$A(x) = B(x) = x^3 + x^2 + 1$;

$B(x) = R(x) = 0$;

$\gcd(A(x), B(x)) = x^3 + x^2 + 1$

$$
\begin{array}{r|l}
 & x^2 + x \\
\hline
x^4 + x^2 + x + 1 & x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
 & \underline{x^6 \quad\quad + x^4 + x^3 + x^2} \\
 & \quad x^5 \quad\quad\quad\quad\quad + x + 1 \\
 & \quad \underline{x^5 \quad\quad + x^3 + x^2 + x} \\
 & \quad\quad\quad x^3 + x^2 \quad\quad + 1
\end{array}
$$

GF(2^3)

		000	001	010	011	100	101	110	111
	+	0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

(a) Addition

		000	001	010	011	100	101	110	111
	×	0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

(b) Multiplication

w	$-w$	w^{-1}
0	0	—
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

(c) Additive and multiplicative inverses

Modular Polynomial Arithmetic

- can compute in field $GF(2^n)$
  - polynomials with coefficients modulo 2
  - whose degree is less than n
  - hence must reduce modulo an irreducible poly of degree n (for multiplication only)
- form a finite field
- can always find an inverse
  - can extend Euclid's Inverse algorithm to find

Table 4.6 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

		000	001	010	011	100	101	110	111
	+	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
001	1	1	0	$x + 1$	x	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$
010	x	x	$x + 1$	0	1	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$
011	$x + 1$	$x + 1$	x	1	0	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2
100	x^2	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$	0	1	x	$x + 1$
101	$x^2 + 1$	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$	1	0	$x + 1$	x
110	$x^2 + x$	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$	x	$x + 1$	0	1
111	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2	$x + 1$	x	1	0

(a) Addition

		000	001	010	011	100	101	110	111
	×	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
010	x	0	x	x^2	$x^2 + x$	$x + 1$	1	$x^2 + x + 1$	$x^2 + 1$
011	$x + 1$	0	$x + 1$	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$	x^2	1	x
100	x^2	0	x^2	$x + 1$	$x^2 + x + 1$	$x^2 + x$	x	$x^2 + 1$	1
101	$x^2 + 1$	0	$x^2 + 1$	1	x^2	x	$x^2 + x + 1$	$x + 1$	$x^2 + x$
110	$x^2 + x$	0	$x^2 + x$	$x^2 + x + 1$	1	$x^2 + 1$	$x + 1$	x	x^2
111	$x^2 + x + 1$	0	$x^2 + x + 1$	$x^2 + 1$	x	1	$x^2 + x$	x^2	$x + 1$

(b) Multiplication

Computational Considerations

- since coefficients are 0 or 1, can represent any such polynomial as a bit string
- addition becomes XOR of these bit strings
- multiplication is shift & XOR
  - cf long-hand multiplication
- modulo reduction done by repeatedly substituting highest power with remainder of irreducible poly (also shift & XOR)

Example

- why mod(x^3+x+1)!!! for gf(2^3)
- in $GF(2^3)$ have (x^2+1) is 101_2 & (x^2+x+1) is 111_2
- so addition is
  - $(x^2+1) + (x^2+x+1) = x$
  - $101 \text{ XOR } 111 = 010_2$
- and multiplication is
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$
    $= x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011.101 = (101){<<}1 \text{ XOR } (101){<<}0 =$
    $1010 \text{ XOR } 101 = 1111_2$
- polynomial modulo reduction (get q(x) & r(x)) is
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - $1111 \bmod 1011 = 1111 \text{ XOR } 1011 = 0100_2$

Summary

- have considered:
  - concept of groups, rings, fields
  - modular arithmetic with integers
  - Euclid’s algorithm for GCD
  - finite fields GF(p)
  - polynomial arithmetic in general and in GF(2^n)