

# 1 GCD Theorems

## 1.1 GCD WR

If  $a$  and  $b$  are integers not both zero, and  $q$  and  $r$  are integers such that  $a = qb + r$ , then  $\gcd(a, b) = \gcd(b, r)$

## 1.2 GCD CT (GCD characterization theorem)

If  $d$  is a positive common divisor of the integers  $a$  and  $b$ , and there exist integers  $x$  and  $y$  so that  $ax + by = d$ , then  $d = \gcd(a, b)$ .

## 1.3 Coprimeness and Divisibility

If  $a, b$ , and  $c$  are integers and  $c \mid ab$  and  $\gcd(a, c) = 1$ , then  $c \mid b$

## 1.4 Primes and Divisibility

If  $p$  is a prime and  $p \mid ab$  then  $p \mid a$  or  $p \mid b$

## 1.5 GCD of One

Let  $a$  and  $b$  be integers. Then  $\gcd(a, b) = 1 \iff ax + by = 1$  where  $x$  and  $y$  are integers.

## 1.6 Division by the GCD

Let  $a$  and  $b$  be integers. If  $\gcd(a, b) = d \neq 0$ , then  $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ .

# 2 EEA

## 2.1 Extended Euclidean Algorithm

If  $a > b > 0$  are positive integers, then  $d = \gcd(a, b)$  can be computed and there exist integers  $x$  and  $y$  so that  $ax + by = d$ .

### 3 Linear Diophantine Equations

Equations with integer co-efficients for which integer solutions are sought.

#### 3.1 Linear Diophantine Equation Theorem, Part 1 LDET1

Let  $\gcd(a,b)=d$ . The linear Diophantine equation  $ax + by = c$  has a solution iff  $d \mid c$

#### 3.2 Linear Diophantine Equation Theorem 2, LDET2

Let  $\gcd(a,b) = d$  where both  $a$  and  $b$  are not zero. If  $x = x_0$  and  $y = y_0$  is one particular integer solution to the equation  $ax + by = d$  then the complete solution is  $x = x_0 + \frac{b}{d}n$ ,  $y = y_0 - \frac{a}{d}n \forall n \in \mathbb{Z}$

### 4 Congruence

Let  $m$  be a fixed positive integer. If  $a, b \in \mathbb{Z}$  we say that  $a$  is congruent to  $b$  modulo  $m$ .  $a \equiv b \pmod{m}$  if  $m \mid (a - b)$ . If  $m \nmid (a - b)$  then  $a \not\equiv b \pmod{m}$

#### 4.1 Equivalence relation

1.  $a \equiv b \pmod{m}$
2. If  $a \equiv b \pmod{m}$  then  $b \equiv a \pmod{m}$
3. If  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$  then  $a \equiv c \pmod{m}$

#### 4.2 properties of congruence

1.  $a + b \equiv a' + b' \pmod{m}$
2.  $a - b \equiv a' - b' \pmod{m}$
3.  $ab \equiv a'b' \pmod{m}$

#### 4.3 Congruences and Division

If  $ac \equiv bc \pmod{m}$  and  $\gcd(c, m) = 1$  then  $a \equiv b \pmod{m}$

## 4.4 Congruent IFF Same remainder

$a \equiv b \pmod{m}$  iff a and b have the same remainder when divided by m.

## 4.5 Modular Arithmetic

### 4.5.1 Congruence class

$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$

$Z_m$  is the set of m congruence classes.  $[a] + [b] = [a + b]$  and  $[a] * [b] = [a * b]$

### 4.5.2 Identity

Something that does nothing.

$\forall a \in S, a * e = a$

### 4.5.3 Inverse

$a * b = b * a = e$  Subtraction is the addition of inverse. Division is multiplication with inverse.

## 4.6 Fermat's Little Theorem

If p is a prime number that does not divide the integer a, then  $a^{p-1} \equiv 1 \pmod{p}$   
For any integer a and any prime p  $a^p \equiv a \pmod{p}$

### 4.6.1 Existence of Inverse

Let p be a prime. if  $[a]$  is any non zero element in  $Z_p$  then there exists an element  $[b] \in Z_p$  so that  $[a] * [b] = 1$

## 4.7 Linear Congruences

$ax \equiv c \pmod{m}$  is a linear congruence. solution if x so that congruence is true.

### 4.7.1 Linear congruence Theorem 1 LCT1

Let  $\gcd(a, m) = d \neq 0$  The linear congruence  $ax \equiv c \pmod{m}$  has a solution iff  $d \mid c$ . Also if  $x_0$  is a solution then complete solution is  $x \equiv x_0 \pmod{\frac{m}{d}}$

### 4.7.2 Linear Congruence Theorem 2, LCT2

Let  $\gcd(a, m) = d \neq 0$ . The equation  $[a][c] = [c]$  in  $Z_m$  has a solution iff  $d \mid c$

### 4.8 Chinese Remainder Theorem

Let  $a_1, a_2 \in Z$  If  $\gcd(m_1, m_2) = 1$  then the simultaneous linear congruences  $n \equiv a_1 \pmod{m_1}$  and  $n \equiv a_2 \pmod{m_2}$  have a unique solution modulo  $m_1 m_2$  Thus is  $n = n_0$  is one integer solution then the complete solution is  $n \equiv n_0 \pmod{m_1 m_2}$

## 5 RSA

### 5.1 Setting up RSA

1. choose two large distinct primes  $p$  and  $q$  and let  $n = pq$ .
2. select an integer  $e$  so that  $\gcd(e, (p-1)(q-1)) = 1$  and  $1 < e < (p-1)(q-1)$
3. solve  $ed \equiv 1 \pmod{(p-1)(q-1)}$  for an integer  $1 < d < (p-1)(q-1)$
4. public key is  $(e, n)$  and private key is  $(d, n)$

### 5.2 sending a message

1. look up public key  $(e, n)$
2. generate an integer message  $M$   $0 \leq M < n$
3. compute the ciphertext  $C$   $M^e \equiv C \pmod{n}$  where  $0 \leq C < n$

### 5.3 receiving a message

1. use the private key  $(d, n)$
2. compute message text  $R$  from  $C$   $C^d \equiv R \pmod{n}$  where  $0 \leq R < n$

## 6 Complex Numbers

**Complex Numbers:** An expression of the  $C = x + yi \mid x, y \in \mathbb{R}$  where  $x$  and  $y$  are real numbers. Has a real and imaginary part.

Mathematical operations  $a + bi = c + di \Leftrightarrow a = c, b = d$   
 $(a + bi) + (c + di) = (a + c) + (b + d)i$   
 $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$

1. Associativity of addition  $(u + v) + z = u + (v + z)$
2. Commutativity of addition  $(u + v) = v + u$
3. additive identity  $0 + 0i$
4. Additive inverse  $-z = -x - yi$
5. Associativity of multiplication  $(u * v) * z = u * (v * z)$
6. Commutativity of multiplication  $(u * v) = v * u$
7. multiplicative identity  $1 = 1 + 0i$
8. multiplicative inverse  $z = x + yi \frac{x-yi}{x^2+y^2}$

### 6.1 Complex conjugate

complex conjugate of  $z = x + yi$  is  $\bar{z} = x - yi$

### 6.2 Modulus

Modulus of  $z = x + yi$   $|z| = |x + yi| = \sqrt{x^2 + y^2}$