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 Diophatine Equations

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

3.1 Linear Diophatine Equation Theorem, Part 1 LDET1

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

3.2 Linear Diophatine 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 $x = x_0 + \frac{b}{d}n$, $y = y_0 - \frac{a}{d}n \forall \epsilon Z$

4 Congruence

Let m be a fixed positive integer. If $a, b \epsilon Z$ we say that a is congruent to b modulo m. $a \equiv bmodm$ if $m \mid (a - b)$. If $m(a - b)$ then $a \neq modm$

4.1 Equivalence relation

$a \equiv bmodm$

If $a \equiv bmodm$ then $b \equiv amodm$

If $a \equiv bmodm$ and $b \equiv cmodm$ then $a \equiv cmodm$

4.2 properties of congruence

$a + b \equiv a' + b'modm$

$a - b \equiv a' - b'modm$

$ab \equiv a'b'modm$

4.3 Congruences and Division

If $ac \equiv bcmodm$ and $gcd(c, m) = 1$ then $a \equiv bmodm$

4.4 Congruent IFF Same remainder

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

4.5 Modular Arithmetic

4.5.1 Congruence class

$[a] = x\epsilon Z \mid x \equiv amodm$
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.
$\forall a\epsilon S, a * e = a$

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 $a^{p-1} \equiv 1modp$
For any integer a and any prime p $a^p \equiv amodp$

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 $[b]\epsilon Z_p$ so that $[a] * [b] = 1$

4.7 Linear Congruences

$ax \equiv cmodm$ 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 $ax \equiv cmodm$ has a solution iff $d \mid c$. Also if x_0 is a solution then complete solution is $x \equiv x_0 mod \frac{m}{d}$

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

5 RSA