NUMBER THEORY FORMULAS

DIVISIBILITY

Divisibility: a

Prime Number
$p > 1$, only factors 1 and p

Composite Number
More than two factors

GCD (HCF): $\gcd(a,b)$

LCM: $\operatorname{lcm}(a,b) = \dfrac{a \times b}{\gcd(a,b)}$

Euclidean Algorithm
$\gcd(a,b) = \gcd(b, a \bmod b)$

EXTENDED EUCLIDEAN

Extended Euclidean
$ax + by = \gcd(a,b)$

Coprime Numbers $(a,b) = 1$

Fundamental Theorem
$n = p_1^a \times p_2^b \times \ldots$

Modular Congruence
$a \equiv b \pmod{n}$

Modular Addition
$(a + b) \bmod n$

Modular Multiplication
$(ab) \bmod n$

MODULAR INVERSE

Modular Inverse: $a^{-1} \bmod n$

Fermat's Little Theorem
Theorem: $a^{p-1} \equiv 1 \pmod{p}$

Euler's Totient $\varphi(n)$

Euler's Theorem
Theorem: $a^{\varphi(n)} \equiv 1 \pmod{n}$

$\varphi(p)$: $p - 1$

$\varphi(p^k)$: $p^k - p^{k-1}$

MULTIPLICATIVE Φ

Multiplicative ϕ
$\phi(ab) = \phi(a)\phi(b)$ if coprime

Chinese Remainder
Solve $x \equiv a_1 \bmod n_1$

Wilson's Theorem
$(p-1)! \equiv -1 \pmod{p}$

Linear Diophantine
$ax + by = c$

Condition
c divisible by $\gcd(a,b)$

Perfect Number
$\sigma(n) = 2n$

MERSENNE PRIME

Mersenne Prime $2^p - 1$

Quadratic Residue
$x^2 \equiv a \pmod{p}$

Legendre Symbol (a/p)

Euler's Criterion
$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

Modular Exponentiation
$a^b \bmod n$

Sum of Divisors
$\sigma(n) = \prod \left[\dfrac{p^{k+1} - 1}{p - 1} \right]$

NUMBER OF DIVISORS

Number of Divisors
$d(n) = \prod (k + 1)$