Definitions

sets are denoted with { ... }

$\mathbb{Z}$ set of all integers {..., -2, -1, 0, 1, 2, ...}

$\mathbb{N}$ set of all natural numbers {0, 1, 2, ...}

\{x} means x is not in the set ie. {1, 2, ...} can be denoted as $\mathbb{N}\backslash\{0\}$

$\in$ - element in set

$\exists$ - there exists

$\forall$ - for all

For $p \in \mathbb{N}$ if p is not prime then it is composite. 0 and 1 are neither prime nor composite

We denote gcd(x,y) simply as (x,y). Note that (x,0) = x.

We denote lcm(x,y) as [x,y]

Recurrence Relations

Given a kth order recurrence of the form $a_n = x_1 a_{n-1} + x_2 a_{n-2} + ... + x_k a_{n-k}$, the closed form is $a_n = C_1 r_1^n + C_2 r_2^n + ... + C_k r_k^n$ where $r_1, r_2, ..., r_k$ are solutions to $r^k - x_1 r^{k-1} - x_2 r^{k-2} - ... - x_k = 0$.

For example fibonacci numbers, $F_n = F_{n-1} + F_{n-2}$, have the characteristic polynomial equation, $r^2 - r - 1 = 0$, and the solutions to the equation are $r = \frac{1+\sqrt{5}}{2}$ and $r = \frac{1-\sqrt{5}}{2}$.

Theorems

Addition, multiplication and subtraction are closed $\forall x$; $x \in \mathbb{Z}$.

The Division Algorithm:

For $\frac{a}{b}$ where $a \in \mathbb{Z}$ and $b \in \mathbb{N}\backslash\{0\}$, there is some quotient $q \in \mathbb{N}$ and remainder $0 \leq r < b$ such that,

$$a = bq + r.$$

i b is said to divide a if $r = 0$. We denote this as $b|a$. If b does not divide a we say $b \nmid a$.

ii When (a, b)=1, a and b are relatively prime

Integer Combination "I.C. Theorem"

If $d|a$ and $d|b$ then $d|(ax+by)$ for $x, y \in \mathbb{Z}$.

Bezout's Theorem:

For $a, b \in \mathbb{Z}$, (a,b) is the smallest positive integer of the form $ax + by$ where $x, y \in \mathbb{Z}$.

Corollary to Bezout's Theorem:

If (a,b)=1 then there exist some $x, y \in \mathbb{Z}$ such that $ax + by = 1$

Euclid's Theorem:

For any integers, $a, b, x : (a, b) = (b, a - bx)$

The Euclidean Algorithm:

$(a, b) = (b, a\text{mod}b)$ where $b < a$

"Important" Theorem:

If $d|ab$ and $(d, a) = 1$ then $d|b$

Prime Importance:

If P is prime and $P|ab$ then $P|a$ or $P|b$.

Corollary to Prime Importance:

If P is prime and $P|a_1a_2...a_n$ then $P|a_k$ for some integer $1 \leq k \leq n$

Fundamental Theorem of Arithmetic:

Every integer a has a unique factorization into primes which can be expressed as $a = \prod P_i^{\alpha_i}$

i a has $\prod(1 + \alpha_i)$ divisors

ii $(a, b) = \prod P_i^{\min(\alpha_i, \beta_i)}$

iii $[a, b] = \prod P_i^{\max(\alpha_i, \beta_i)}$

Modular Arithmetic

Congruence: a is congruent to b mod m, denoted $a \equiv_m b$, if $m|a - b$.

Congruence satisfies equivalence relations so it has the following properties:

Reflexive: $a \equiv_m b$

Symmetric: if $a \equiv_m b$ then $b \equiv_m a$

Transitive: if $a \equiv_m b$ and $b \equiv_m c$ then $a \equiv_m c$

(Modular arithmetic) If $a \equiv_m b$ then,

$a + c \equiv_m b + c$

$ac \equiv_m bc$

$a^n \equiv_m b^n$ for $n \in \mathbb{N}$

Cancellation Theorem:

Let $(a, m) = 1$. If $ax \equiv_m ay$ then $x \equiv_m y$.

Theorem:

Let $(a, m) = d$. If $ax \equiv_m ay$ then $x \equiv_{\frac{m}{d}} y$.

Inverse:

If $(a, m) = 1$ then a has an inverse mod m such that $ax \equiv_m 1$. Additionally x is unique mod m since $ax \equiv_m 1$ and $ay \equiv_m 1$ implies $x \equiv_m y$ by the cancellation theorem.

Corollary:

Given a prime number p and an integer n such that $n < p$ then n has an inverse mod p.

Wilson's Theorem:

Given a prime number p then $(p - 1)! \equiv_p p - 1 \equiv_p -1$

Fermat's Theorem:

Given a prime number p then $a^{p-1} \equiv_p 1$ or $a^p \equiv_p a$

Euler's Totient Function:

$\phi(n)$ is the number of integers in $\{1, 2, ..., n\}$ that are relatively prime to n.
$\phi(n) = n(1 - 1/P_1)(1 - 1/P_2)...(1 - 1/P_k)$ where $P_1, P_2, ..., P_k$ are prime factors of n.
Additionally, if n is prime then $\phi(n) = n - 1$

Euler's Theorem:

If $(a, m) = 1$ then $a^{\phi(n)} \equiv_m 1$