MATH2988 - Number Theory and Cryptography

Definitions

1 Divisibility

Let $a, b \in \mathbb{Z}$. We say that a divides b if there exists $d \in \mathbb{Z}$ such that:

$$b = d \cdot a$$

Notation: a divides b, $a|b$

2 Greatest Common Divisor

Let $a, b \in \mathbb{Z}$. An integer d is called a common divisor of a and b if $d|a$ and $d|b$.
An integer g is called the greatest common divisor if it is the greatest integer with this property, ie:

$$\text{gcd}(a, b) := max \{d \in \mathbb{Z} : d|a,\ d|b\}$$

By convention, $\text{gcd}(0, 0) = 0$

3 Coprime

If $\text{gcd}(a, b) = 1$ then a and b are called coprime or relatively prime numbers.

4 Prime and Composite

Let $n \in \mathbb{Z}$, $n > 1$, n is called prime if all of its divisors are 1 and n. Otherwise it is called composite.

Remark: 0 and 1 are neither prime nor composite.

Notation: The set of primes is $\mathbb{P}$

5 The Modulus

Let $m \in \mathbb{Z}$. We say that a is congruent to b modulo m if:

$m|b - a$
or $b = a + km$ for some $k \in \mathbb{Z}$
or a and b have the same residues (remainders) modulo m.

Notation: $a \equiv b \pmod{m}$

6 Congruence Classes

Let $m \in \mathbb{Z}, a \in \mathbb{Z}^+$. The congruence class of $a \equiv b \pmod{m}$ is the set of integers which are congruent to a modulo m. There are always m congruence classes.

7 Complete System

A complete system of residues modulo m is a set of integers containting exactly one representative from each congruence class modulo m.

The standard complete system is:

$$\{0, 1, 2, ..., m - 1\}$$

8 Reduced System

A reduced set of residues modulo m is a set of integers containing exactly one element from each invertible congruence class modulo m. (Congruence class of a with $\gcd(a,m)=1$).

The standard reduced set is:

$$\{a \in \mathbb{Z} \mid 0 \le a \le m-1,\ \gcd(a,m)=1\}$$

9 Euler's Phi-Function

The size of a reduced set of residues is called Euler's phi-function of m, $\varphi(m)$.

10 Order

Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ with $\gcd(a,m)=1$. The order of $a \equiv b \pmod{m}$ is the smallest $j \in \mathbb{Z}^+$ such that:

$$a^j \equiv 1 \pmod{m}$$

Notation: $\mathrm{ord}_m(a)$

11 Multiplicative Functions

A function $f : \mathbb{Z}^+ \to \mathbb{Z}$ is called multiplicative if for all $n, m \in \mathbb{Z}^+$ with $\gcd(n,m)=1$, $f(mn) = f(m) \cdot f(n)$.

f is called completely multiplicative if it holds for all pairs m and n.

12 Liouville Function

$$\lambda(n) := (-1)^{\#\text{of primes in the factorisation of n}}$$

$\lambda(n)$ is completely multiplicative.

n	1	2	3	4	5	6	7	8	9	10
factorisation of n	1	2	3	2^2	5	$2 \cdot 3$	7	2^3	3^2	$2 \cdot 5$
$\lambda(n)$	1	-1	-1	1	-1	1	-1	-1	1	1

13 Möbius Function

$$\mu(n) := \begin{cases} \lambda(n) & \text{if } n \text{ is square-free} \\ 0 & \text{otherwise} \end{cases}$$

$\mu(n)$ is completely multiplicative

n	1	2	3	4	5	6	7	8	9	10
factorisation of n	1	2	3	2^2	5	$2 \cdot 3$	7	2^3	3^2	$2 \cdot 5$
$\lambda(n)$	1	-1	-1	0	-1	1	-1	0	0	1

14 Square Free

$n \in \mathbb{Z}^+$ is called square-free if for any prime p, $p^2 \nmid n$

15 Tau Function

$\tau(n)$ is the number of positive integer divisors of n.

$$\tau(n) = \sum_{d \mid n} 1$$

16 Sigma Function

$\sigma(n)$ is the sum of positive integer divisors of n.

$$\sigma(n) = \sum_{d|n} d$$

17 Perfect Numbers

n is called perfect if it equals the sum of all its proper divisors (all divisors except n), ie:

$$n = \sigma(n) - n \quad \text{or} \quad 2n = \sigma(n)$$

18 Mersenne Primes

Primes of the form $2^k - 1$ are called Mersenne Primes.

19 Multiplicative Functions at Powers of Primes

$$\begin{aligned}
\varphi(p^k) &= p^k - p^{k-1} \\
\tau(p^k) &= k + 1 \\
\sigma(p^k) &= \frac{p^{k+1} - 1}{p - 1} \\
\lambda(p^k) &= (-1)^k
\end{aligned}$$

20 Big O Notation

Let $f(k), g(k)$ be two positive valued functions over positive (integer) numbers.
We say that "$f(k)$ is O($g(k)$)" if:
There are positive numbers N, C such that

$$f(k) \leq C(g(k)) \quad \text{for all k} \geq \text{n}$$

21 Polynomial Time

An algorithm is said to be of polynomial time if there exists positive a such that the number of bit operations required for the algorithm with the length of input $\leq k$ is O(k^a).