Sets

Alvin Lin

Discrete Math for Computing: January 2017 - May 2017

Divisibility and Modular Arithmetic

Floor function: $\lfloor x \rfloor : \mathbb{R} \to \mathbb{Z}$:

x	$\lfloor x \rfloor$
4.5	4
4.99	4
4.1	4
4	4
12.8	12
-3.14	-4

Division Algorithm

For any integer a and a positive integer d, there is a unique quotient q and a unique remainder r so that $a = dq + r$ and $0 \leq r < d$.

a	d	$a(\text{div } d) = q$	$a(\text{mod } d)$
23	5	4	3
2017	12	168	1
18	7	2	4
-10	6	-2	2

Applications of the Mod Function

1. Hashing Functions: A rudimentary hashing function can take the form of $h(x) = x(\text{mod } d)$.

2. Pseudorandom Sequences: Given some seed value a_0, a pseudorandom sequence can be generated using the sequence $a_{n+1} = (ax_n + b)(\text{mod } d)$.

3. Basic Cryptography: The mod function is applied for basic cryptographic schemes like the Caesarshift cipher.

Mod Congruency

1. $d \equiv 0 \pmod{d}$

2. $a \equiv a + kd \pmod{d}$

3. $a \equiv a - kd \pmod{d}$

4. $a \equiv b \pmod{d}$ *if* $(a - b)$ *is a multiple of* d

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech