Definitions (Module Ø3)

Integer division - division where input and output are always integers

Linear combination of two numbers is the sum of multiples of those numbers

ex: a linear combination of x and y would be $ax + by$ where a, b are integers

Division algorithm - states that the quotient and the remainder are unique. For a number n.

$n = qd + r$ where $d > 0$, $0 \leq r \leq (d-1)$, n is an integer

Quotient of n is equal to $q = n \text{ div } d$ where $d > 0$ and div is integer division

Remainder of n is equal to $r = n \bmod d$ where $d > 0$ and mod is the modulus operation

mod m is a function that takes an integer X as input and outputs $X \bmod m$ (where m is also an integer)

addition mod m - operation where the sum is calculated and then mod m is applied on the sum

ex: $x + y \bmod m$ is $(x+y) \bmod m$

multiplication mod m - operation where the product is calculated and then mod m is applied on the product

ex: x times y mod m is $(xy) \bmod m$

ring - the closed mathematical system created by mod m. Contains m elements and is denoted by $\mathbb{Z}_m$. $\{0, 1, \ldots, m-1\}$

ex $\mathbb{Z}_6 \equiv \{0,1,2,3,4,5\}$

congruence mod m = let x and y be two integers such that x mod m = y mod m If x mod m = y mod m, then x is congruent to y mod m and denoted

$x \equiv y \pmod{m}$

prime number - a number greater than 1 whose factors are only 1 and itself

composite number - a number that has factors in addition to 1 and itself

prime factorization - the product of the prime numbers that make up an integer, where the integer is >1 (in non-decreasing order)

The Fundamental Theorem of Arithmetic - the fact that every integer > 1 has a unique prime factorization

Non-decreasing sequence - a sequence in which each number is equal to or greater than the one that came before

ex: 1,1,2,3,17 counter-ex: 1,1,3,2,17

Multiplicity of a prime factor is the # of times that prime factor appears in a number's prime factorization Can be expressed via exponential notation