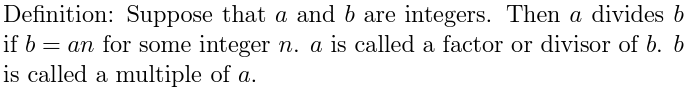
Chapter 4-[Number Theory](https://mfleck.cs.illinois.edu/building-blocks/version-1.3/number-theory.pdf)

Wednesday, December 28, 2022

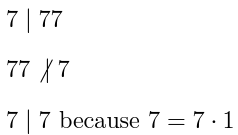
1:27 AM

***Number Theory:***

Divisibility:

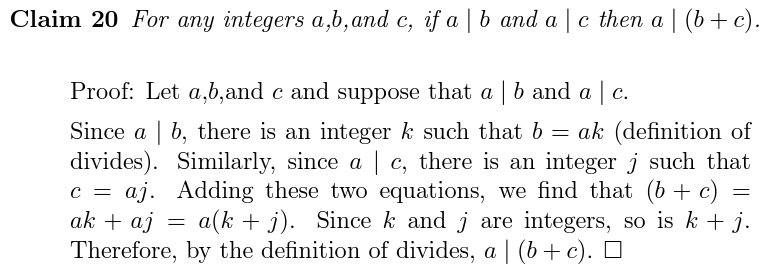








***Proof with divisibility:***



*Try to keep proofs using only integers, construct math from the ground up, this helps prevent errors.*

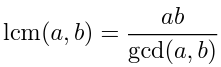
*Notice that k | (a - b) if and only if k | (b - a).*

**Fundamental Theorem of Arithmetic**: Every integer can be written as the product of one or more prime factors. Except for the order in which you write the factors, this prime factorization is unique.

For example, 260 = 2\*2\*5\*13 and 180 = 2\*2\*3\*3\*5.

Zero is neither prime nor composite, there **infinitely many** ways to factor 0.

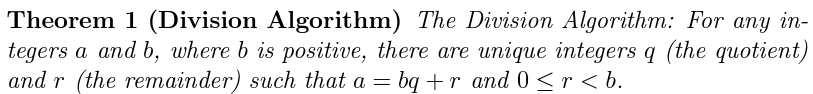
**Formula for Least Common Multiple (lcm):**



Where gcd is the Greatest Common Divisor function.

(use the *Euclidean Algorithm*, or manually inspect two numbers' prime factorizations and extract shared factors to find gcd)

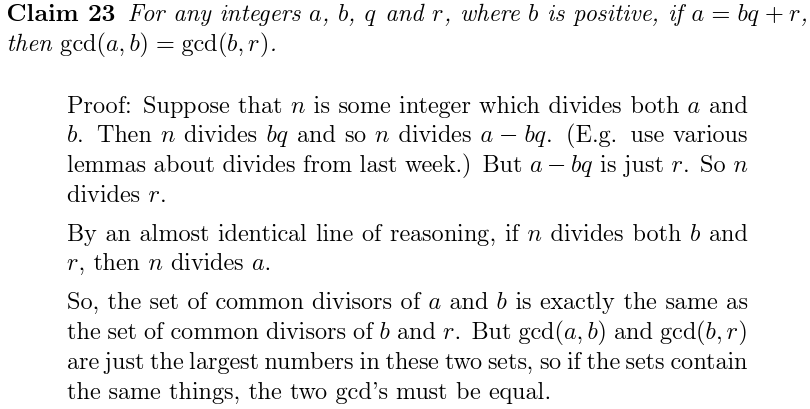
When two integers a and b share no common factors, then gcd(a,b) = 1. The two integers are called **Relatively Prime**.



**Remainder is required to be non-negative!**

*So -10 divided by 7 has the remainder 4, because -10 = 7\*(-2)+ 4.*

*(don't be like me and forget how to do basic division)*



*(to prove the 2 have the same common divisors, we just need to prove that given x|a and x|b, we can get x|r and x|b (and vice versa), so the two sets are the same)*

**Corollary** means that a fact is a really easy consequence of a previous claim.

*(in the above case, concluding that gcd(a,b) and gcd(b,r) are the same from the proven claim-the set of common divisors of (a,b) is the exact same as the set of common divisors of (b,r)-is a corollary)*

In *Modular Arithmetic*, there are only a finite set of numbers, addition “wraps around” from the highest number to the lowest one.

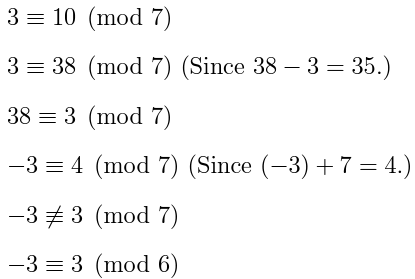
***Congruence Mod K:***

Two integers are “congruent mod k” if they differ by a multiple of k.

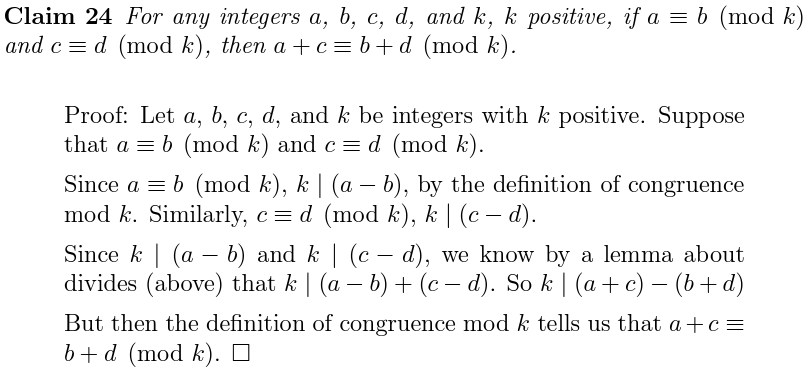
Formal Definition:



*Examples:*



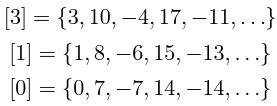
***Modular Arithmetic Proof:***



***Congruence Class/Equivalence Class:***

The equivalence class of x (written [x]) is the set of all integers congruent to x mod k. (with k being fixed and x being the variable)

For example, if k is fixed to be 7,



Modular Congruence Rules:

