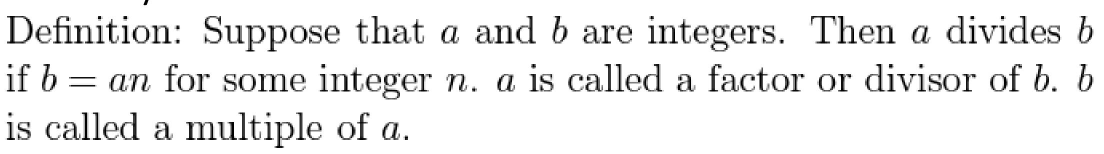
Chapter 4-Number Theory

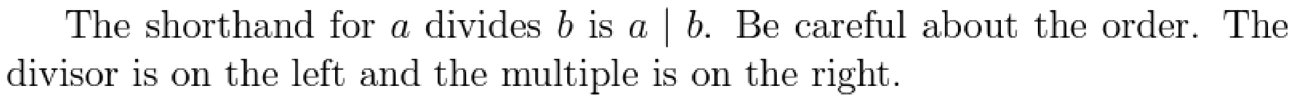
Wednesday, December 28, 2022
1:27 AM

Number Theory:

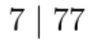
Divisibility:



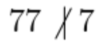
Definition: Suppose that a and b are integers. Then a divides b if $b = an$ for some integer n. a is called a factor or divisor of b. b is called a multiple of a.



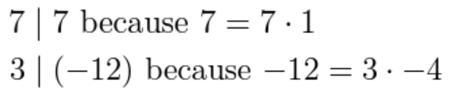
The shorthand for a divides b is $a \mid b$. Be careful about the order. The divisor is on the left and the multiple is on the right.



$7 \mid 77$



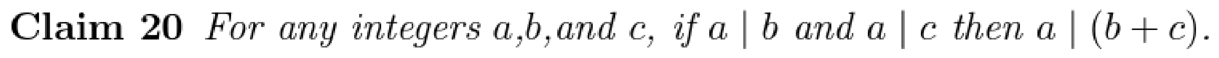
$77 \nmid 7$



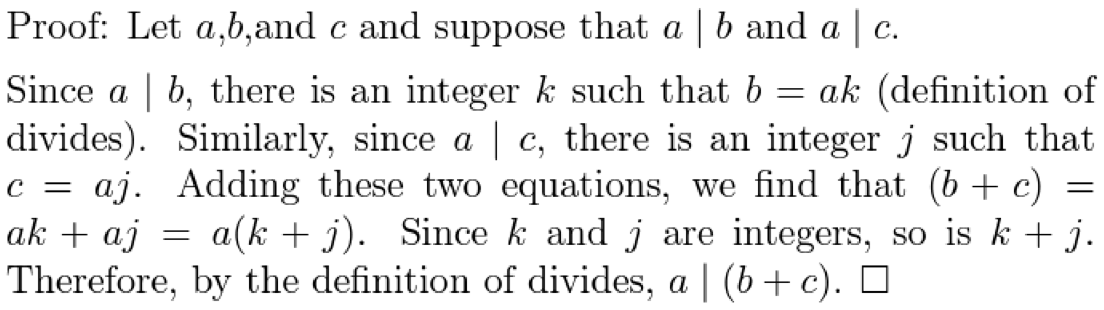
$7 \mid 7$ because $7 = 7 \cdot 1$

$3 \mid (-12)$ because $-12 = 3 \cdot -4$

Proof with divisibility:



Claim 20 *For any integers a,b,and c, if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.*



Proof: Let a,b,and c and suppose that $a \mid b$ and $a \mid c$.

Since $a \mid b$, there is an integer k such that $b = ak$ (definition of divides). Similarly, since $a \mid c$, there is an integer j such that $c = aj$. Adding these two equations, we find that $(b + c) = ak + aj = a(k + j)$. Since k and j are integers, so is $k + j$. Therefore, by the definition of divides, $a \mid (b + c)$. □

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.

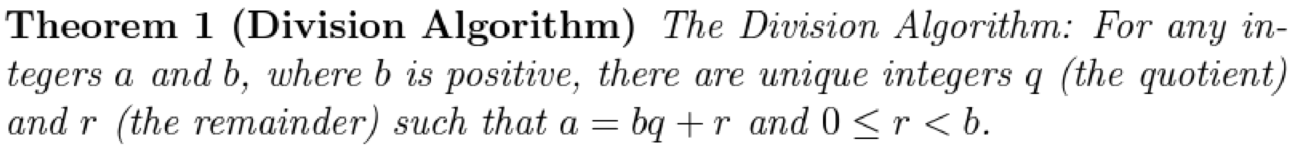
Zero is neither prime nor composite, there **infinitely many** ways to factor 0.

Formula for Least Common Multiple (lcm):

$$\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$$

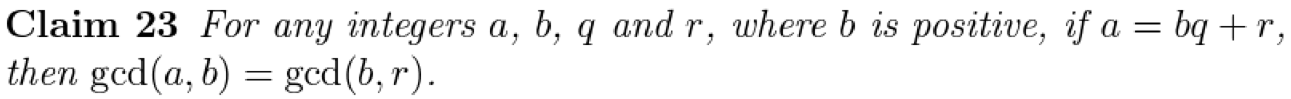
Where gcd is the Greatest Common Divisor function.
(use the *Euclidean Algorithm*, or manually inspect two numbers' prime factorizations and extract shared factors to find gcd)

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

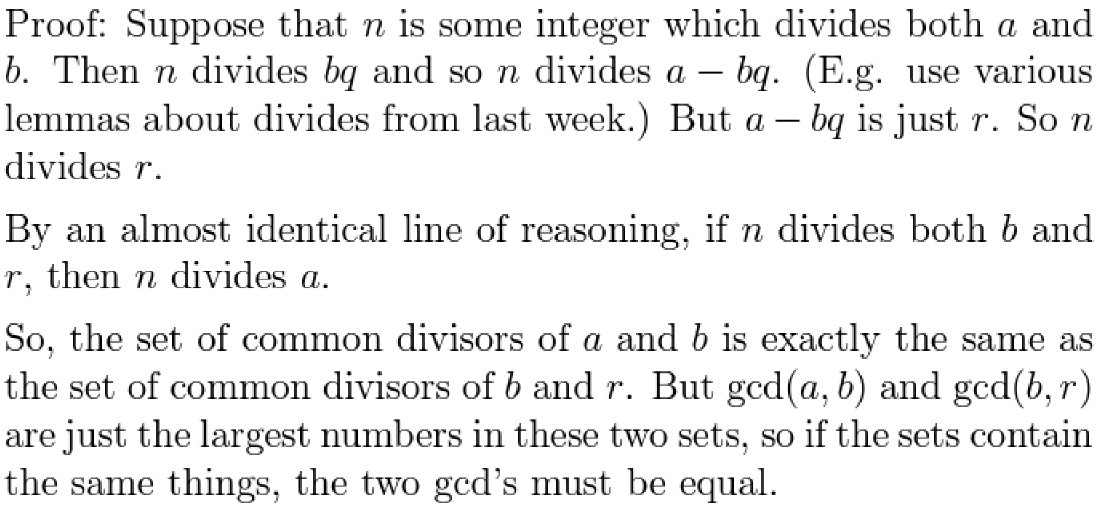


Theorem 1 (Division Algorithm) *The Division Algorithm: For any integers a and b, where b is positive, there are unique integers q (the quotient) and r (the remainder) such that $a = bq + r$ and $0 \leq r < b$.*

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)



Claim 23 *For any integers a, b, q and r, where b is positive, if $a = bq + r$, then* $\gcd(a,b) = \gcd(b,r)$.



Proof: Suppose that n is some integer which divides both a and b. Then n divides bq and so n divides $a - bq$. (E.g. use various lemmas about divides from last week.) But $a - bq$ is just r. So n divides r.

By an almost identical line of reasoning, if n divides both b and r, then n divides a.

So, the set of common divisors of a and b is exactly the same as the set of common divisors of b and r. But $\gcd(a,b)$ and $\gcd(b,r)$ are just the largest numbers in these two sets, so if the sets contain the same things, the two gcd's must be equal.

(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)

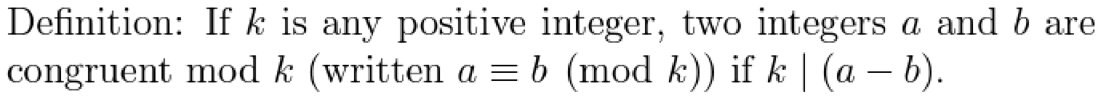
Corollary means that a fact is a really easy consequence of a previous claim.
(in the above case, concluding that gcd(a,b) and gcd(b,r) are the same from the proven claim-the set of common divisors of (a,b) is the exact same as the set of common divisors of (b,r)-is a corollary)

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:

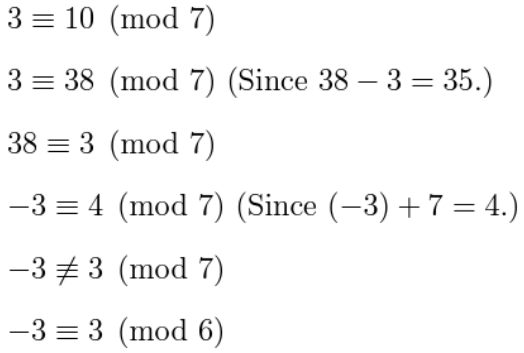
Two integers are "congruent mod k" if they differ by a multiple of k.

Formal Definition:



Definition: If k is any positive integer, two integers a and b are congruent mod k (written $a \equiv b \pmod{k}$) if $k \mid (a - b)$.

Examples:



$3 \equiv 10 \pmod{7}$

$3 \equiv 38 \pmod{7}$ (Since $38 - 3 = 35$.)

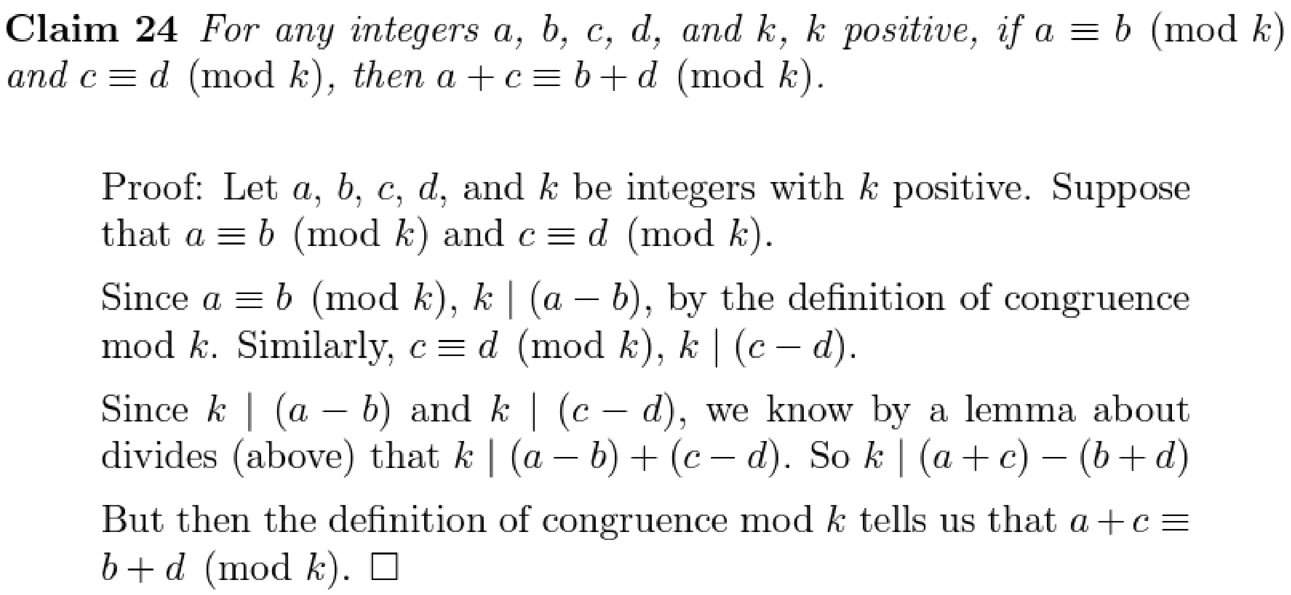
$38 \equiv 3 \pmod{7}$

$-3 \equiv 4 \pmod{7}$ (Since $(-3) + 7 = 4$.)

$-3 \not\equiv 3 \pmod{7}$

$-3 \equiv 3 \pmod{6}$

Modular Arithmetic Proof:



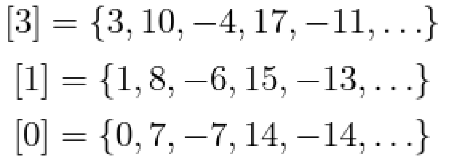
Claim 24 *For any integers a, b, c, d, and k, k positive, if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$, then $a + c \equiv b + d \pmod{k}$.*

> Proof: Let a, b, c, d, and k be integers with k positive. Suppose that $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$.
>
> Since $a \equiv b \pmod{k}$, $k \mid (a - b)$, by the definition of congruence mod k. Similarly, $c \equiv d \pmod{k}$, $k \mid (c - d)$.
>
> Since $k \mid (a - b)$ and $k \mid (c - d)$, we know by a lemma about divides (above) that $k \mid (a - b) + (c - d)$. So $k \mid (a + c) - (b + d)$
>
> But then the definition of congruence mod k tells us that $a + c \equiv b + d \pmod{k}$. □

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,

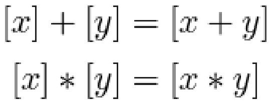


$[3] = \{3, 10, -4, 17, -11, \ldots\}$

$[1] = \{1, 8, -6, 15, -13, \ldots\}$

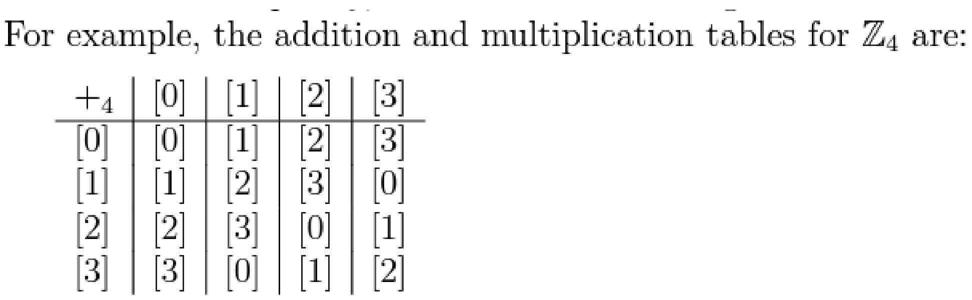
$[0] = \{0, 7, -7, 14, -14, \ldots\}$

Modular Congruence Rules:



$[x] + [y] = [x + y]$

$[x] * [y] = [x * y]$



For example, the addition and multiplication tables for $\mathbb{Z}_4$ are:

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\times_4$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]