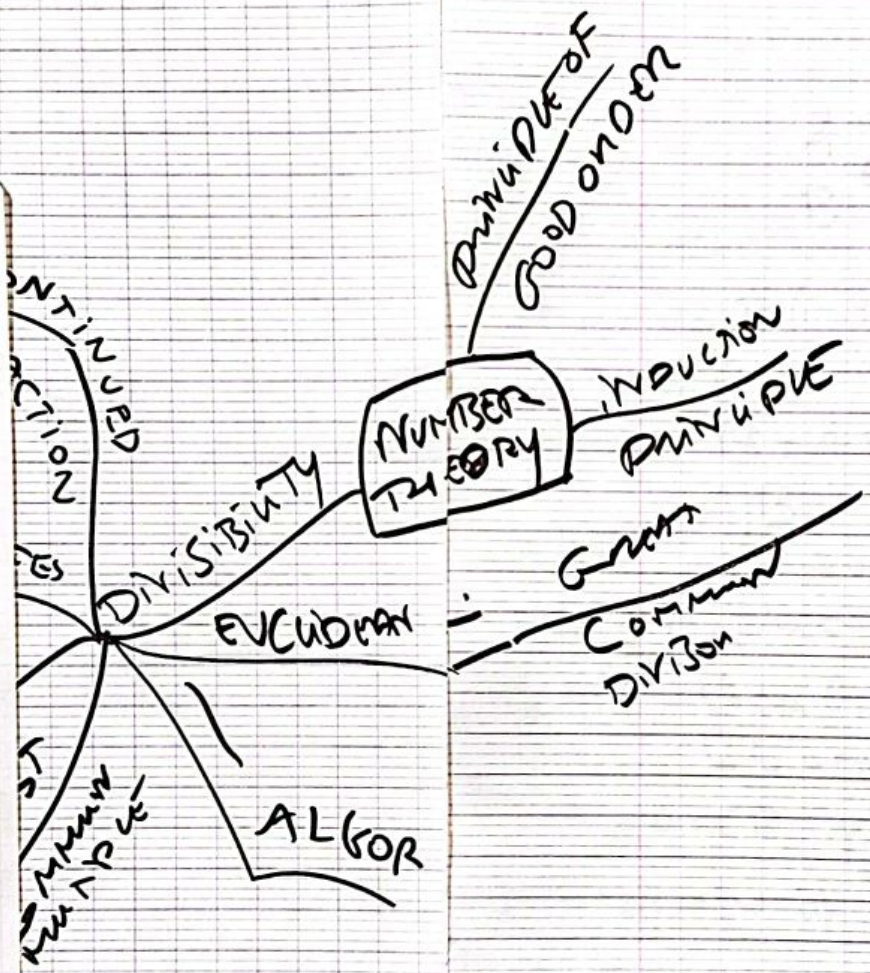
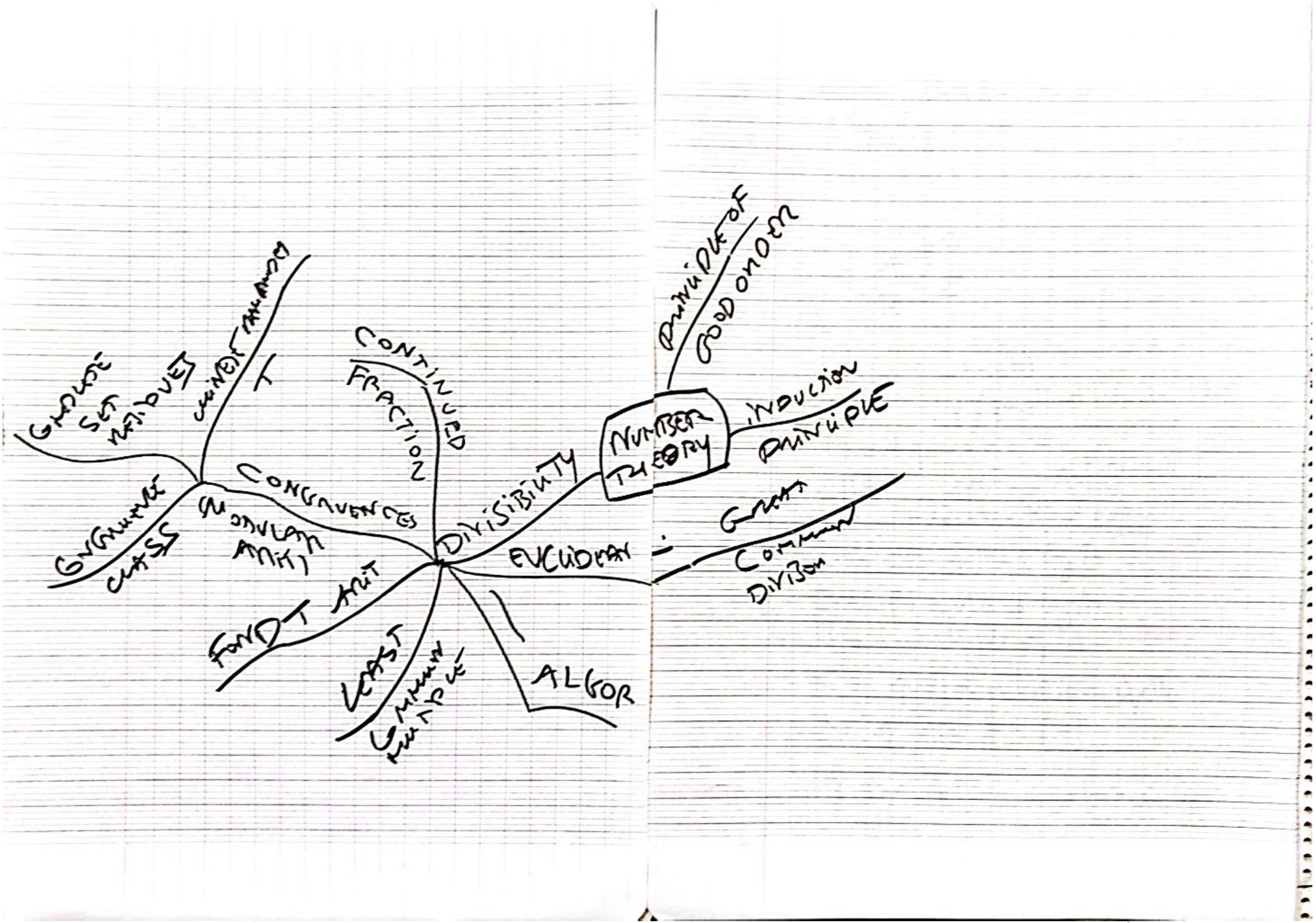


1502 NUMBER THEORY

Scanné avec CamScanner



Scanné avec CamScanner

NB THEORY — algebraic
— computational

Principle of good order

$S \subset \mathbb{N}$

non empty $\Rightarrow$ contains a smallest element

"Archimedean property"

"division"

$\forall a, b \in \mathbb{N}$, $a \neq 0$, there is at least one positive int n such that $n \cdot a \geq b$

...

induction principle

Let S be a set of $\mathbb{N}$ who has the following 2 properties

P1 $1 \in S$

P2 if $k \in S$, then $k+1 \in S$

then $S = \mathbb{N} \setminus \{0\} = \mathbb{N}^*$

T Given now $B = \mathbb{N}^* \setminus S$

we want to prove that

$B = \emptyset$

Proof

Ex $A \neq 0$, $A \in \mathbb{Z}$, B

Divisibility

A divides B (without rest)

if there is an int q (quotient) such that

$B = Aq$

$A \mid B$ not $\rightarrow A \nmid B$

i.e. Reduction / opera

A is the divisor of the $\div$ by B

if $A \mid B$ B can be divided by A

B is a multiple of A

$1 \geq A < B$ proper division of B

$A \mid 0$ regardless of $A \in \mathbb{Z} \setminus \{0\}$

T if $A \mid B$ then $A \mid BC$ whatever $C \in \mathbb{Z}$

Scanné avec CamScanner

Commence

T ∀ A|B and B|C Then A|C

A|B1 A|B ⇒ A|C

A|B A|C

A|(Bx+Cy) ∀x,y ∈ ℤ

A|B B|A A = ±B

Euclidean division

euclidean division quotient remainder can be generalized to relative int & polynomials

D or "integer ÷"

B by A stopping when rest < than A

"relatively prime"

T A B ∈ ℤ

∨

0

there are unique int q quotient

r remainder

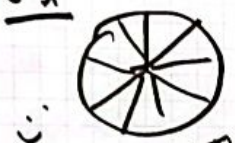
B = Aq + r ⇔ B − Aq = r

$\mathcal{R}_{\equiv}$ equiv R

0 ≤ r < A

∀ A ≠ B then 0 < r < A

EX

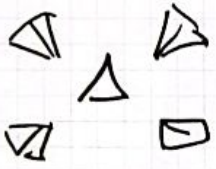


B PART A

impossible with one part remaining

r = 1

such as q = 2



non zero

10 = 2.4 + 1

∈ ℤ B = Aq + r

0 ≥ r < |A|

∀ A ≠ B then 0 < r < |A|

Scanné avec CamScanner

Greatest Common Divisor factor

GCD (gcd)

when at least one of them is not zero, is the largest +ve int that divides the numbers without a remainder

highest common factor / greatest common measure / highest common divisor

D $a, b \in \mathbb{Z}$ $ab \neq 0$

gc of a and b (a,b)

is the +ve int n that satisfies the following:

P1 $d|a$ and $d|b$ (n without remainder n is the +)

P2 If $c|a$ and $c|d$ then $c \leq d$ and $c|d$ by def

1 always c d

36 54 ↪ a common divisor is a +ve int that divides 36 and also 54 for ex 1 or 2

$D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

$D_{54} = \{1, 2, 3, 6, 9, 18, 27, 54\}$

$Div_{36} \cap Div_{54} = \{1, 2, 3, 6, 9, 18\}$

max → $= 18$

that not all prime always ∃

Bézout's T $a, b \in \mathbb{Z}$ $ab \neq 0$

If d divides a and b then there exist ? int x and y such that

$d(a,b) =$ exactly

Euclidean Division Lemma

R3 hidden ≃ concepts of ≠ levels

$\overline{R}_{\equiv}$ equiv R

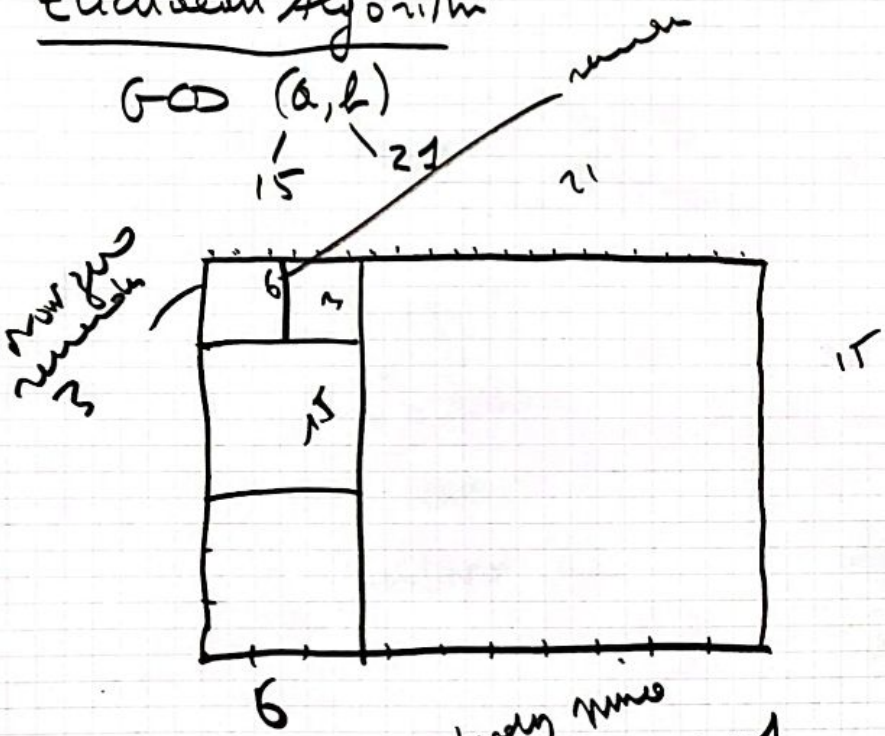
OR

if $a, b \in \mathbb{Z}$ $ab \neq 0$

then $S = \{ax + by \mid x, y \in \mathbb{Z}\}$

Euclidean Algorithm

GCD (a, b)



L

C

Multiple

LCD

ex

35

$M_3 \{3, 6, 9, \ldots\}$

$M_5 \{5, 10, 15 \ldots\}$

$\{15, 30, 45, 60\} \ldots = 15$

min

Fond T ~~existence~~ unit

every natural nbr $n > 1$ can be written as product of prime numbers except for the order in which the prime factors are arranged

ex 223 ...

Scanné avec CamScanner

R3 hidden ≃ concepts of ≠ levels

$\mathcal{R}_{\equiv}$ equiv R

Congruence (modulo arit)

"modulus"

7:00 → 3:00 8 hours

7+8 ≠ 15

"wrap around" every 12 Hrs

17:00 → 5:00 7 hrs

hub ant modulo 12

17 is congruent not only to 12 itself but also to 0

So the time "17:00" can also be written as "0:00"

Since 17 is congruent to 0 modulo 12

D $m \in \mathbb{Z} \setminus 0$

If a & b leave the same remainder when divided by m in euc ÷

a is congruent to b modulo m

~~$a \equiv b \bmod m$~~ $a \equiv b \bmod a(m)$

there are at least one rel int such that

$a = b + km$

residue = int cong to another modulo + given int m

$m \mid (a-b)$

R1 ⇒ null remainder for ÷

R2 exclude in addition to 0 also $1 - 1$

Scanné avec CamScanner

R3 hidden = concepts of ≠ levels org of abstrac°

- modulus of a and b are cong mod m if they have the same remainder in euc ÷ by m
  their diff is a multiple of m

- oriented angles
  "2 meas are cong mod 2π [rad]
  iff their diff is a multiple of 2π [rad]
  2 meas of the same angle

- alg cong mod I in a com ring
  ↳ an ideal

"x is cong to y mod I iff their diff belongs to I
= equiv ∝ R compatible with + and × → possibility def a quotient ring of the parent set with its ideal I

- same = similar
  ample equiv R or set plane fig

$\mathcal{R}_{\equiv}$ equiv R
$a, b, c, m \in \mathbb{Z}$ $m > 1$

R $a \equiv a \bmod(m)$

S $a \equiv b \bmod(m) \Leftrightarrow b \equiv a \bmod(m)$

T $a \equiv b,\ b \equiv c \Rightarrow a \equiv c$

= equality however
multiple°

- ex
  $2.1 \equiv 2.3 \bmod(4)$ $2+1 \not\equiv 3 \bmod(4)$
  ↳ or a change of modulus

P1 If $a \equiv b \bmod(m)$ and $d \mid m$ then $a \equiv b \bmod(d)$
P2 —— & $a \equiv b \bmod(s)$ then a and b cong mod [n, s]
... ↑

Congruence class

mod sub cong class
subset of the set $\mathbb{Z}$ defined by the $\mathcal{R}_{\equiv}$
that 2 elts $a, b \in \mathbb{Z}$ are in the same class
a iff $a \equiv b \bmod(m)$ ...

Scanné avec CamScanner

Ex $m = 3$

÷ set of int into cong classes mod 3

$[a]_m := a \bmod (m)$

Complete set of residues

Reduced residue sys

Euler's totient function