18/4/2020

Video

(5)

2.8 Greatest common Division :- gcd

Let a and b are any two integers in which at least one is non-zero. Then the greatest common divisor of a and b denoted by gcd(a, b) or [a, b] is positive integer d such that

(i) d|a and d|b
(ii) If c|a and c|b then c ≤ d

ex — gcd(8, 12) = 4 and
gcd(10, 15) = 5 and gcd(a, b) = a If a|b.

2.9 Euclid's Algorithm

The gcd of two integers a and b can be determined by a process known as Euclid's algorithm which is as follows:

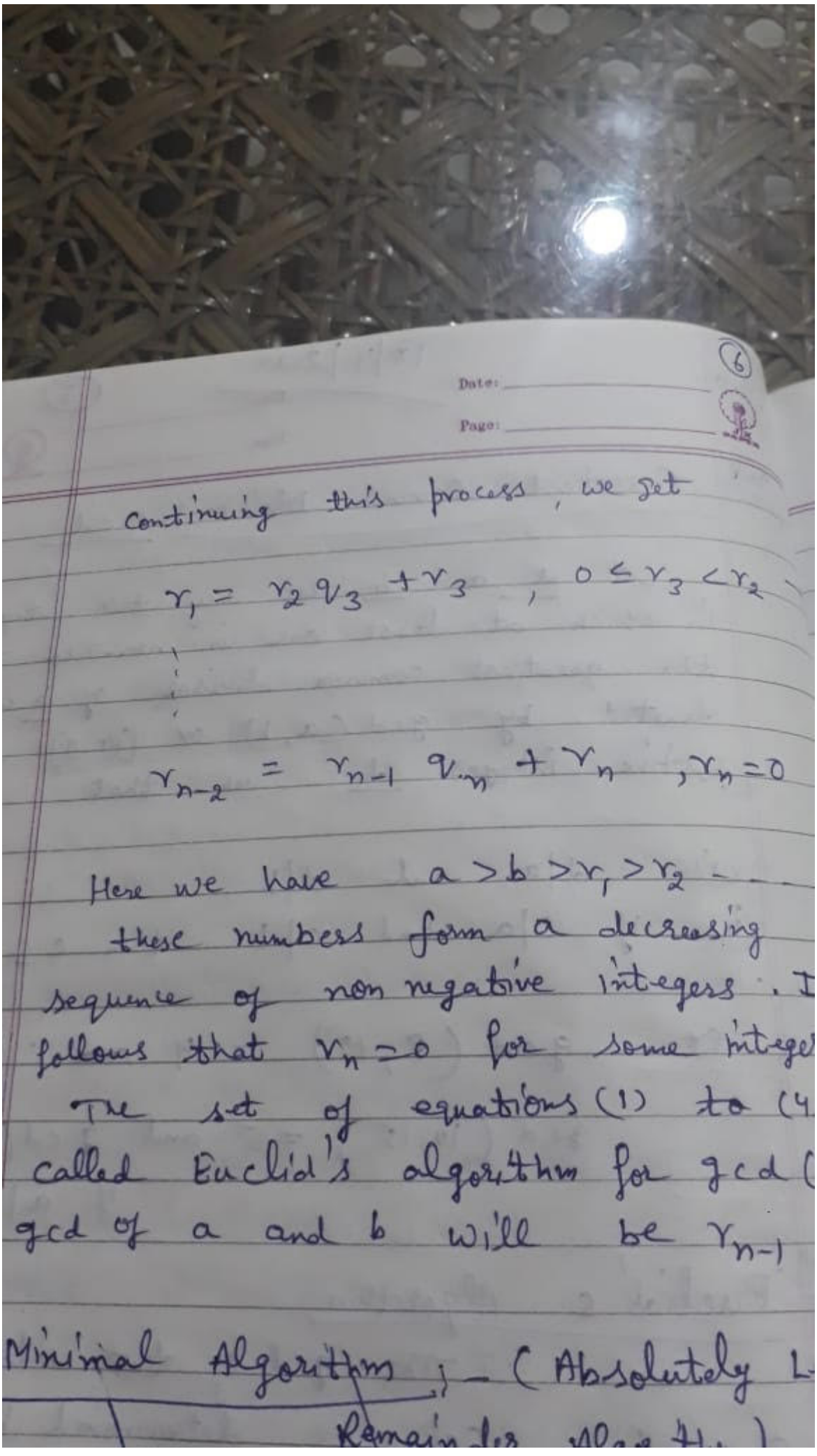
Let a and b both positive and a > b. Then there exist integers q_1 and r_1 such that

$$a = bq_1 + r_1, \quad 0 \le r_1 < b \qquad (1)$$

(division alg)

again there exist integer q_2 and r_2 such that

$$b = r_1 q_2 + r_2, \quad 0 \le r_2 < r_1$$



Date:

Page:

Continuing this process, we get

$$r_1 = r_2 q_3 + r_3 \quad , \quad 0 \le r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n \quad , r_n = 0$$

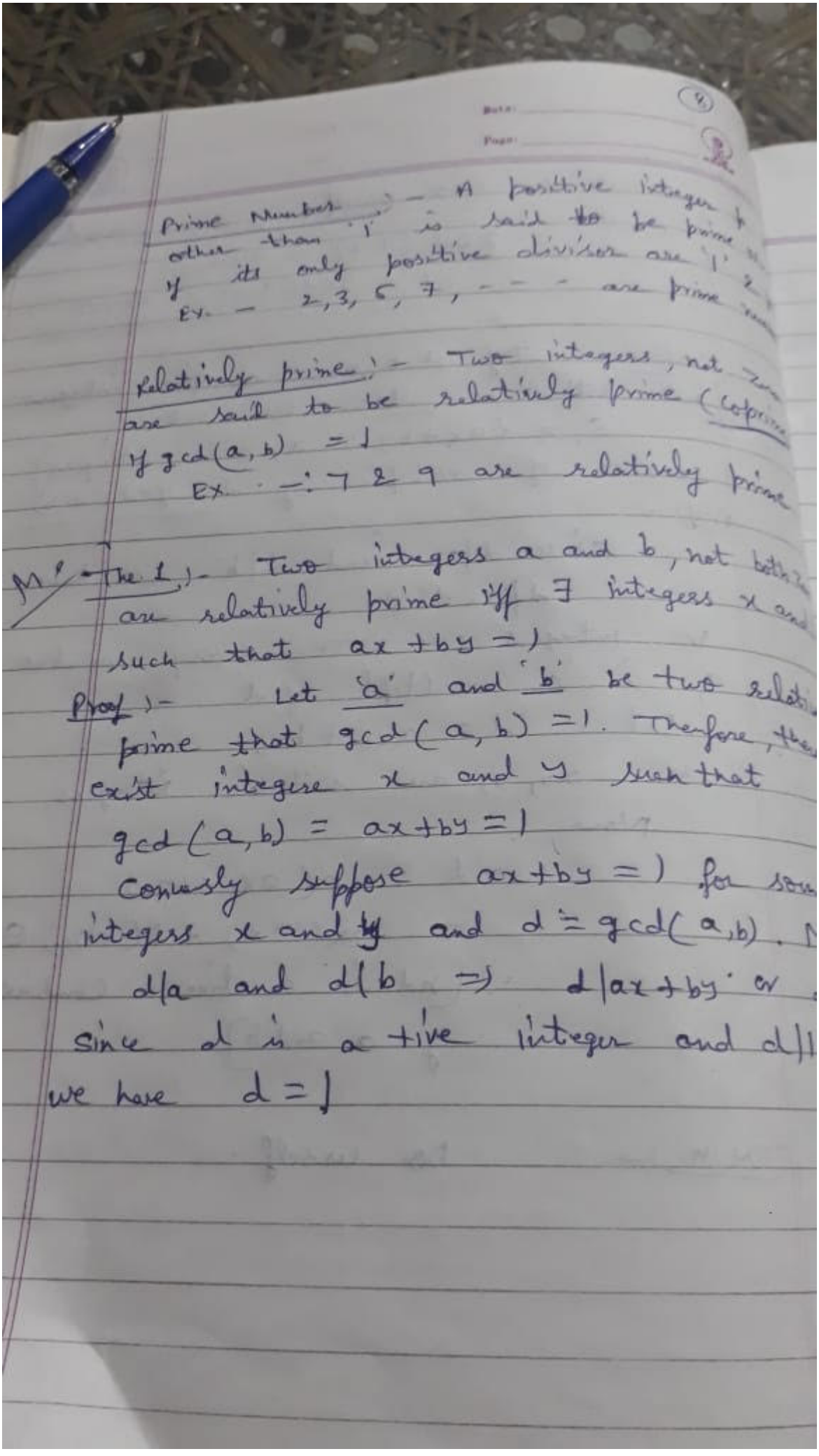
Here we have $a > b > r_1 > r_2 \ldots$

these numbers form a decreasing sequence of non negative integers. I follows that $r_n = 0$ for some integer

The set of equations (1) to (4 called Euclid's algorithm for gcd (gcd of a and b will be r_{n-1}

Minimal Algorithm :- (Absolutely L

Remainder



Prime Number :- A positive integer p other than '1' is said to be prime if its only positive divisor are '1' & p.
Ex. - 2, 3, 5, 7, - - - are prime numbers.

Relatively prime :- Two integers, not zero are said to be relatively prime (coprime) if gcd(a, b) = 1
Ex. :- 7 & 9 are relatively prime

Th. 1 :- Two integers a and b, not both zero are relatively prime iff ∃ integers x and y such that ax + by = 1

Proof :- Let 'a' and 'b' be two relatively prime that gcd(a, b) = 1. Therefore, there exist integers x and y such that
gcd(a, b) = ax + by = 1
Conversly suppose ax + by = 1 for some integers x and y and d = gcd(a, b). Now
d|a and d|b ⇒ d|ax + by or
since d is a +ive integer and d|1
we have d = 1