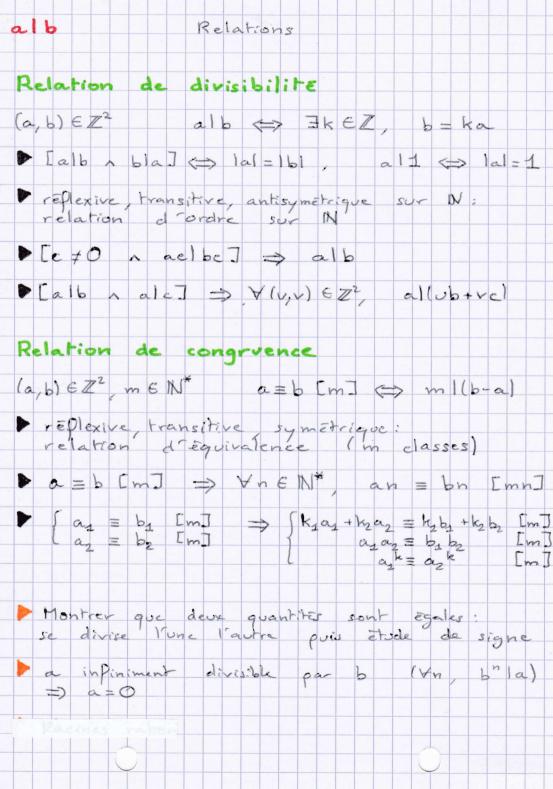
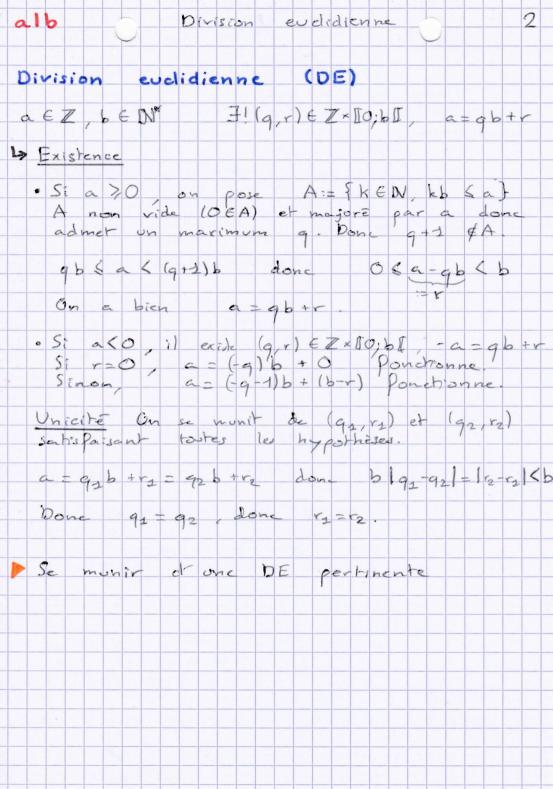
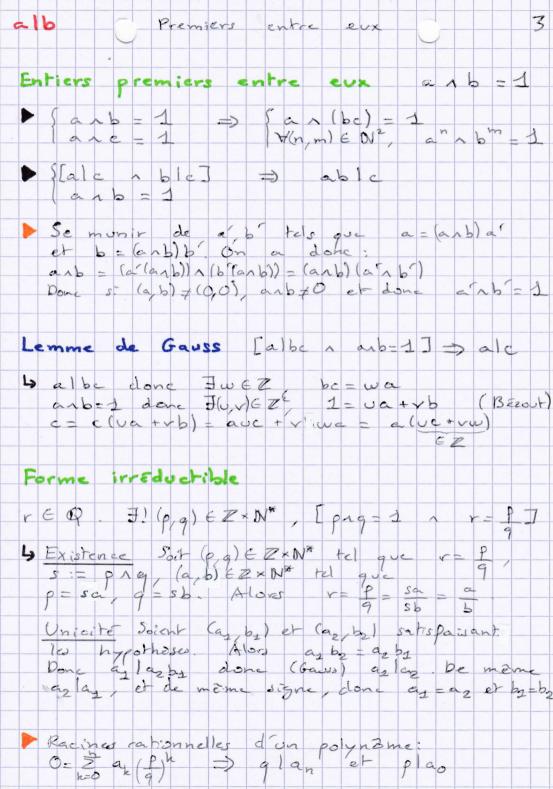
-		-		
	0		b Presentation	1
	5			
			A .: N	
1			Arithmétique	
		•	Presentation 1	
			Relations 1	
		9	1 Letanons	•
		•	Division evolidienne 2	-
			Plus grand diviseur common 2	)
		(80	Premiers entre eux 3	
			The second of th	
	-		BEZOUT 3	
		•	BEZOUT 3	
		0	Plus petit common multiple 4	
			Generalisation 4	
		0.	Nombres premiers 5	
			Nombres premiers 5	
	+ 11			
	-			
-				
	1			
	-	10	abre de pages: 5	





alb PGCD Plus grand diviseur commun (PGCD)  $(a,b) \in \mathbb{Z}^2$ .  $\exists 1 p \in \mathbb{N}$ ,  $-p \mid a \in \mathbb{Z}$ ,  $\exists 1 p \in \mathbb{N}$ ,  $-4q \in \mathbb{Z}$ ,  $\exists 1 p \in \mathbb{N}$ ,  $\exists 1 p \in \mathbb{N}$ , b Existènce and = bna = lalalbl: on sippor elab? Récurrence forte sur atb. Ho vrate (p=0 vévific toute les hypothèses). Soit n & W. Si atb=n+2, a > b et t; vrate pour tout i & n - Soit b=0: p-a fonctionne - Soit b > 0: on & mount de p=(a-b) n b qui existe par hypothèse. p fonctionne Unicité pa et pa verificant les hypothèses se divient l'un l'autre donc sont égaux. Raisonner par recurrence sur a+b Dan0 = 1al an1 = 1 Danb=0 ( ) [a=0 1 b=0] ► (ke) 1 (kb) = 1 kl (anb) ► anb=an(b+ka) Yk € Z (perturbation Algorithme d'Euclide Utiliser and : b n (a mod b). Successivement. Le premier terme est strictement décroissant à partir de la devaidne itération d'où la terminaison. Exemple: 147,105=105,42 = 42,21 = 21,0=21



alb BEZOUT Relation de Bézout (a,b) & Z2 3 (v,v) & Z2, va+vb = a 1 b Con se ramène à (ab) GN2 Récurrence

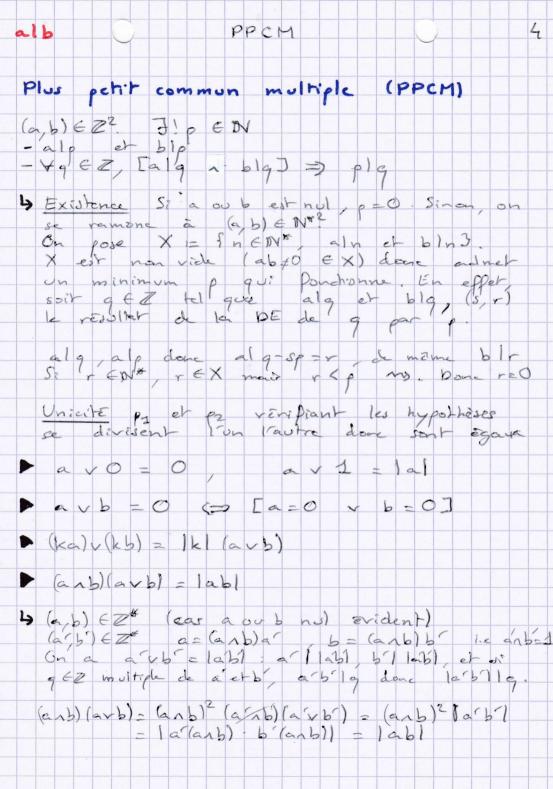
Porte sur a+b Ho voic; (0,0) fonctionne
Soit n EN. Si a+b=n+2 a 2b Hi vrais

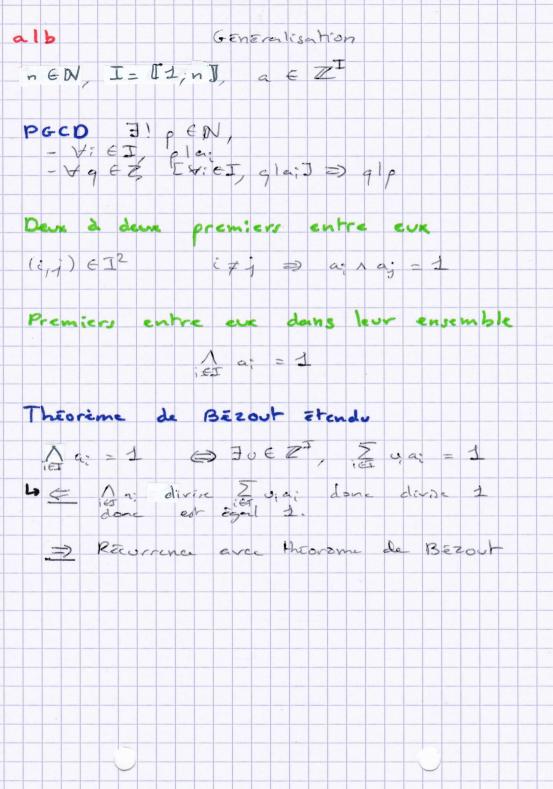
pour tout i (n: 120) ponctionne (anb=a)

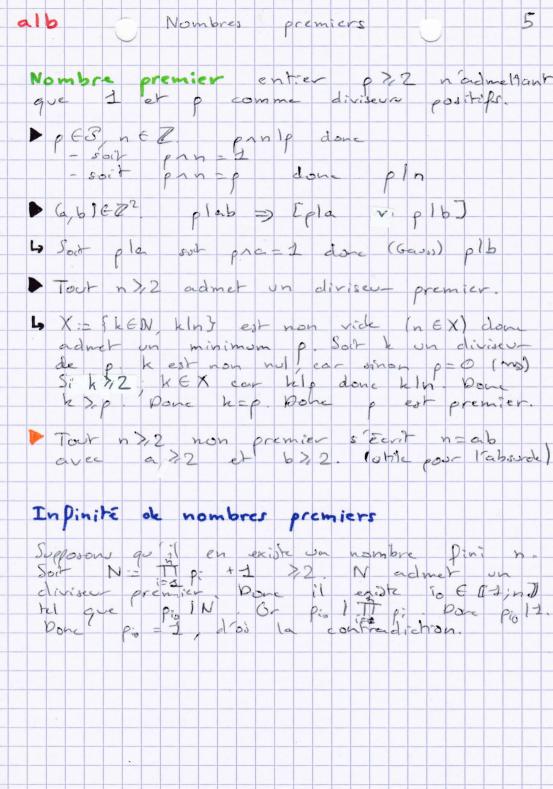
- Si - b=0: (10) ponctionne (anb=a)

- Sinon anb=(a-b)nb donc un couple

pouchonne par hypothèse Peut s'obtenir par remontée de l'algorithme d'Eudide L'ensemble des solutions s'obtient par théorème de superposition et Gauss. De monit de lo,v/ tel que va+vb=anb Théorème de Bézout anb = 1 ( ) ( ) ( ) ( ) ( ) ( ) ( ) 4 => donné par relation de 18 Ezout E and divise a et b done vatbr=1







alb Petit Héorème de Fermat p/m => mp-2 = 1 [p] pES, mEZ 4 (a,b) E 22 = a + b P [p] EZ Hi = " nf = n [p]" Ho varie Soit n EN Si Ha varie (n+1) f = n p + d = n + d [p] par hy other Done Hans. Soit m E Z\* O = (-m+m) f = (-m) f + m f = -m + m f [p]. Soit m EZ tol que pt m ice pr m = 1 con p ES pl m (mp-1-1) done (Gauss) pl(mp-1) ie mp=11/4 Décomposition en produit de Pacteurs premiers n E Z 3! (0, r,p,x) E 5-1, 23 x N x 3 5 5 7 3 x N x 65, 7 3 n = v II più où les pi sont distincts Existence Recurrence sor n & N noce 0 = 3 pois
extension à 2° avec 0 = 1. Its voice (produit vol)
Soit n & N Si It: voice visin, soit n+1 est premiter
soit il s'écrir neab avec a, b & (2: n), d'o)
le réputer par hypothère Unicité Fastidieuse n E Zo p E 3. Val (n) = max sx EN, paln Valuations ny ln2 ( ) V 0 ( 3, Valp (ny) & Valp (n2) Vp 6 3, { Valp (n2 nn2) = min (Valp (ny), Valp (nz), Valp (ny), Valp (ny), Valp (ny), Valp (ny) (n1,n2) EZO.