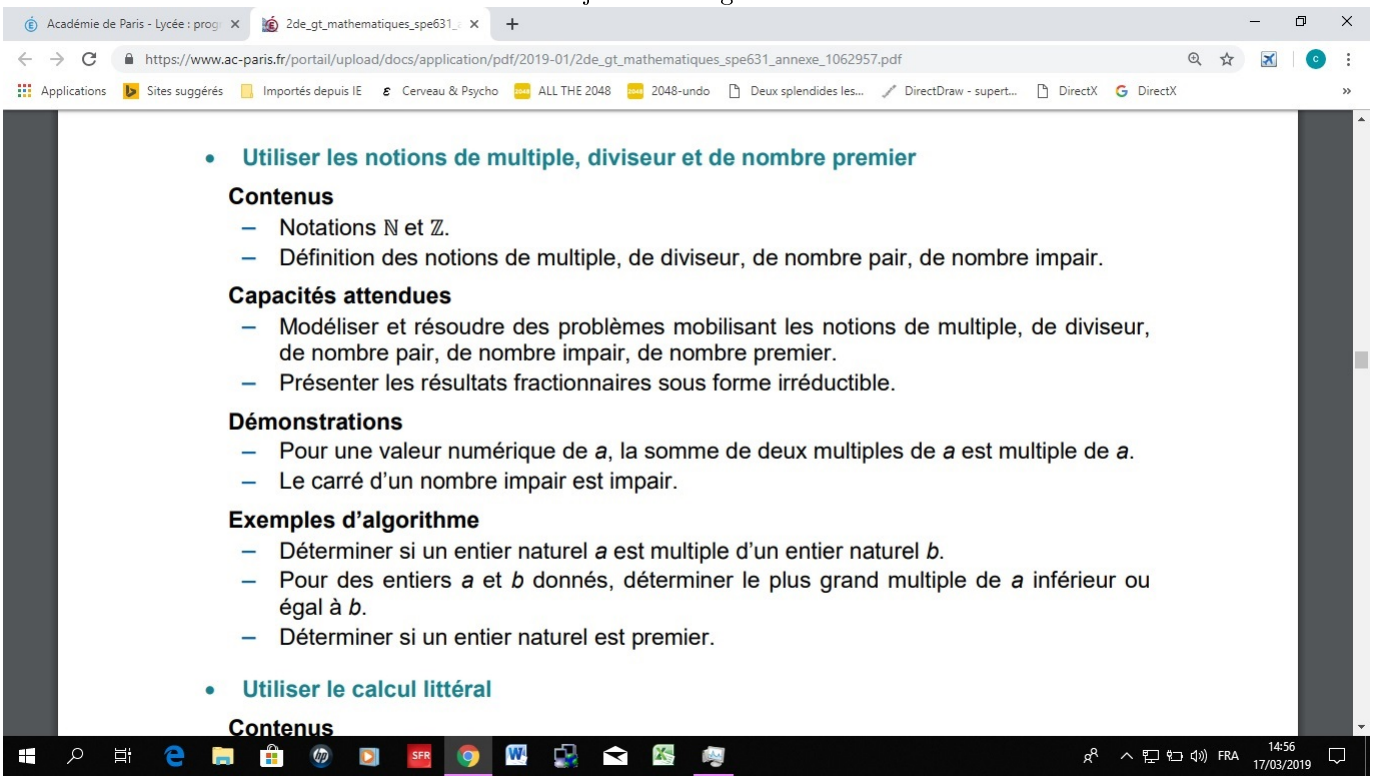
1 Introduction

Disposant d'un logiciel, je ovus tape directement le cours froid plutôt que vous le faire mettre dans votre cahier. Vous pouvez l'imprimer et le coller si vous voulez (ce n'est pas une obligation, il restera en ligne de toute façon). C'est même mieux de le laisser et de vérifier les versions MAJ où j'aurai corrigé les fautes.



2 L'ensemble le plus célèbre

A priori, c'est une notion première, mais je vous en donne une définition (qui est hors-programme). De toute façon, elle repose sur une autre notion première.

Abréviation provisoire (ne pas l'apprendre): << A est une partie inductive de $\mathbb{R}$ >> abrège << $0 \in A$ et pour tout nombre x : si $x \in A$ alors $x + 1 \in A$ >>

<< $\mathbb{N}$ >> est une abréviation de << ensemble des nombres qui peuvent dire *je suis dans toutes les parties inductives de* $\mathbb{R}$ >>

Les programmes n'étant pas cohérents, vous ne serez informés qu'en Terminale de l'axiome que vous êtes autorisés à utiliser dès la seconde. Il s'appelle *axiome de récurrence*. Il ne fait que reprendre la définition ci-dessus. Donc elle n'est pas forcément inutile. Cerise sur le gâteau, vous utiliserez (toujours cette incohérence) l'axiome de récurrence en ... première (toujours sans en recevoir l'information officielle) au moment de croire aux formules donnant le terme général de certaines suites célèbres (appelées suites arithmétiques et suites géométriques)

note humoristique: la réciproque est vraie, à savoir que les formules que vous apprendrez en première surles suites IMPLIQUENT l'axiome de récurrence: ce ne sont donc pas des "petits cas particuliers superficiels". A bon entendeur, je donne souvent en défi fastement rémunéré de le prouver.

2.1 Phonétique

$\mathbb{N}$ s'appelle l'ensemble des entiers naturels. L'ensemble $\mathbb{Z} := \{x \mid x \in \mathbb{N} \text{ ou } (-x) \in \mathbb{Z}\}$ s'appelle l'ensemble des entiers relatifs.

Ce n'est pas mis dans la copie d'écran, mais c'est utilisé dans certains DST de mes collègues, la tradition est de vous donner aussi la définition des ensembles très célèbres suivants:

$\mathbb{Q} := \{x \mid \text{il existe } y \in \mathbb{N} \text{ tel que } y \neq 0 \text{ et } xy \in \mathbb{Z}\}$

$\mathbb{D} := \{x \mid \text{il existe } y \in \mathbb{N} \text{ tel que } x \times (10^y) \in \mathbb{Z}\}$

$\mathbb{D}$ se prononce *ensemble des nombres décimaux* et $\mathbb{Q}$ se prononce *ensemble des nombres rationnels*

3 Autres définitions (révisions de collège)

<< a est un diviseur de b >> abrège << li existe $x \in \mathbb{Z} : ax = b$ >>

<< a est un multiple de b >> abrège << b est un diviseur de a >>

<< a est un nombre premier>> abrège << le cardinal de l'ensemble des diviseurs positifs de a est 2 >>

4 Oublis du programme sur le mot impair

Un nombre entier est dit impair quand il n'est pas pair (vous le savez déjà). Il est dit pair quand il est un multiple de 2. Jusque là, tout va bien. Hélas, le programme oublie que (je l'ai testé au moins 600 fois jusqu'en L2) ça semble être un exercice très difficile de prouver la chose suivante:

Pour tout nombre entier impair a, il existe un nombre entir n tel que $a = 2n + 1$

Du coup, il exisge que nous vous prouvions que tout nombre impair a un carré impair, très probablement parce que la personne qui a écrit ces lignes s'est trompée en pensant que << impair>> voulait dire << de la forme $2n + 1$ avec $n \in \mathbb{Z}$ >>.

Ceci étant dit, $(2p+1)^2 = 2(2p^2+2p)+1$ (pour tout nombre p, et c'est vérifiable en 5ième. Si p est un nombre entier, en divisant $2(2p^2 + 2p) + 1$ par 2, vous obtiendrez $(2p^2 + 2p) + 0.5$, c'est à dire un nombre entier auquel on ajouté 0.5.

5 Une preuve commandée par le programme

$a(u+v) = au+av$ pour tous les nombres. Donc pour tous nombres entiers u, v, a le nombre entier $a(u+v)$ est un multiple de a. En classe, je vous prouverai le théorème suivant en utilisant cette idée.

Théorème: la somme de deux multiples de a est un multiple de a

Aussi évident que ça puisse paraitre, vous pouvez lire comme moi dans la copie d'écran que c'est demandé. Par contre, formellement, il y a une petit jonglage de deux quantificateurs qui nécessite de le faire en face à face.

6 Les "algos"

..démandés par votre programme, car c'est de ça qu'il s'agit sont les suivants:

let $r := 0$ in while $r + a \leq b$ do $r := r + a$ done renvoyer r
renvoie le plus grand multiple de a qui ne dépasse pas b. Là encore, c'est une évidence intuititve d'école primaire, mais exigée.

let $r := 0$ in while $r + a \leq b$ do $r := r + a$ done ; if $r = b$ then répondre "b est un multiple de a"> else répondre "b"> n'est pas un multiple de a"
Sans commentaire, je vous interrogerai...

Pour la troisième demande, c'est une blague. Ca a été durant 100ans, un problème de recherche très avancée de trouver un algorithme RAPIDE qui permet de savoir si un nombre est premier ou non (on en a trouvé officiellement un en 2003.

Actuellement, on ne sait toujours pas s'il existe des algorithmes rapides pour factoriser les nombres entiers et la plupart des systèmes de cryptage du monde sont basés sur le pari qu'il n'en existe pas.

En fait, votre programme compte sur une culture "pédagogique" de l'enseignant, qui veut que ça veut dire *dites leur bien de ne pas essayer tous les diviseurs, mais de s'arrêter quand on a atteint un nombre dont le carré dépasse a.* Du coup je vous écris "docilement" cet algorithme. Mais attention, il faut savoir qu'il ne s'agit là que d'un snobisme. En effet, ou bien on pense aux ordinateurs comme des "outils magiques" et dans ce cas c'est la méthode et évidente à laquelle vous pensez qui est valable. Ou bien on est payé 5000 euros par mois comme codeur et on cherche des programmes qui marchent "en théorie" mais aussi qui "tournent vite". Cette demande du programme est assez étrange puisqu'elle demande de vous informer d'un tout petit détail d'optimisation. Que vous trouveriez vite tous seuls pour les personnes concernées de toute façon par cette étude. Si vous venez de passer 34 minutes à chercher des diviseurs de 2711 et que vous n'en avez pas trouvé, et qu'au moment de faire une pause, vous en êtes rendu à 60, je ne connais pas grand monde qui va avoir la bêtise de continuer, vu que $60 \times 60 = 3600$ et dépasse 2711.

let $x := 2$ in let $r := true$ in while x pas diviseur de a et $x^2 \leq a$ do $x := x + 1$ done; if x diviseur de a then $false$ else $true$

répond à la question << a est-il premier?>>

7 Autres trucs non écrits dans programme

La fonction récursive suivante vous donne le pgcd de (a, b).

pgcd(a,b) := if $a = 0$ then b else if $a > b$ then $pgcd(b, a)$ else $pgcd(a, b - a)$

Avant c'était enseigné au collège. PGCD veut dire "plus grand commun diviseur"