Sur quelques questions d'arithmétique

0. Prérequis.

Dans ce qui suit, j'utilise le raisonnement par absurde et minimalité. Ce mode de raisonnement a pour fondement le fait que $\mathbf{N}$ est bien ordonné, i.e. que toute partie non vide de $\mathbf{N}$ a un plus petit élément. Le principe de ce raisonnement est le suivant. Pour montrer qu'une propriété portant sur les entiers est vraie, on suppose qu'elle ne l'est pas. Il y a donc un ensemble non vide de contre-exemples. On choisit alors le plus petit contre-exemple et on tente d'aboutir à une contradiction. C'est essentiellement la même chose que la méthode de descente infinie, qui consiste, à partir d'un contre-exemple, à en produire un plus petit et à recommencer, mais je trouve que c'est un peu plus simple à mettre en œuvre.

1. Deux variantes du pgcd.

On définit le *pgcd* de deux entiers $a, b \geq 0$ non tous deux nuls, comme le plus grand diviseur commun (au sens de l'ordre usuel) de $\mathbf{N}$. On a la proposition suivante :

Proposition 1.
Si d est le pgcd de a et b et si δ est un diviseur de a et b, alors δ divise d.

Démonstration. On note d'abord que le cas où a ou b est nul est trivial. On raisonne par l'absurde et minimalité en choisissant un contre-exemple a, b, avec $a \leq b$, tel que a soit le plus petit possible et b le plus petit pour a fixé. On a $a > 0$. On considère alors a et $b - a$. Il est clair que les diviseurs communs à a et b sont les mêmes que ceux de a et $b - a$. En particulier, on a $d = pgcd\,(a, b) = pgcd\,(a, b - a)$ et δ divise aussi a et $b - a$. Mais, comme $b - a$ est $< b$, le couple $(a, b - a)$ (ou $(b - a, a)$ si $b - a < a$) n'est plus un contre-exemple en vertu de l'hypothèse de minimalité. Il en résulte que δ divise d et on a gagné.

Remarques 2.
1) On notera que l'astuce de cette démonstration (remplacer a, b par $a, b - a$) est très proche de l'algorithme d'Euclide.
2) On peut aussi montrer la proposition en utilisant la division euclidienne de d par δ, mais ce n'est pas plus simple.
3) Avec ce lemme, on a facilement le théorème de Gauss (on regarde $pgcd(ac, bc)$) et donc l'unicité de la décomposition en produit de facteurs premiers.

2. Un contre-exemple.

Dans ce paragraphe, je donne un exemple où le résultat de la proposition 1 ne subsiste pas dans le cas d'un anneau totalement ordonné mais pas bien ordonné.

Je considère l'anneau $A = \mathbf{R}[T^2, T^3]$. Il s'agit du sous-anneau de $\mathbf{R}[T]$ formé des polynômes sans terme de degré 1 en T. On ordonne $\mathbf{R}[T]$ (et donc A) en définissant, pour $P(T) = \sum_{i=1}^{n} a_i T^i$ avec $a_n \neq 0$, $P(T) > 0 \Longleftrightarrow a_n > 0$. Sur les monômes, cet ordre coïncide avec celui des degrés.

On considère alors, au sens de cet ordre, $pgcd\,(T^5, T^6)$. Je dis que c'est T^3. Il est clair qu'il divise et que les diviseurs communs dans A (qui le sont aussi dans $\mathbf{R}[T]$) ne peuvent être que les T^i, avec $0 \leq i \leq 5$. On voit que $1, T^2, T^3$ sont des diviseurs communs, (car on a $T^5 = T^2 \times T^3$ et $T^6 = T^3 \times T^3 = T^2 \times T^2 \times T^2$), mais pas T (il n'est pas dans A) ni T^4 ni T^5 (toujours à cause de l'absence de T). Mais alors T^2 divise T^5 et T^6 mais ne divise pas T^3.

Remarques 2.
1) L'anneau A, s'il est totalement ordonné, n'est pas bien ordonné car il contient des suites strictement décroissantes : $T^2, T^2 - 1, \cdots, T^2 - n, \cdots$.
2) On sait que cet anneau n'est pas intégralement clos donc pas factoriel. En effet, l'élément T, qui n'est pas dans A, est dans le corps des fractions de A (car on a $T = T^3/T^2$) et entier sur A (car il est racine de $X^2 - T^2 = 0$).

3. À propos de l'ordre de présentation.

Après avoir écrit ce qui précède pendant mes vacances vosgiennes, j'ai retrouvé l'article de Samuel à Orsay dans ses œuvres complètes. Contrairement à ce que je disais, ce n'est pas dans le bulletin de l'APMEP, mais dans l'Enseignement Mathématique (revue suisse), T. XIII, fasc. 3, 1967, p. 223-231, je te l'envoie par courrier. Ce qu'il dit est très intéressant, mais très marqué "maths-modernes" (si tu connais mon Cours d'Algèbre tu verras que j'ai été très influencé, jadis, par ce texte de Samuel). En particulier, l'ordre qu'il propose et qui commence par *pgcd*, *ppcm* s'appuie sur la principalité des idéaux de $\mathbf{Z}$. Je crois maintenant, très fermement, que c'est une erreur pédagogique et épistémologique de parler trop tôt d'idéaux, je peux m'expliquer plus là-dessus si tu le souhaites.
Tu verras aussi que la démonstration que je donne ci-dessus de la prop. 1 n'est pas très éloignée de celle de Zermelo pour l'unicité de la décomposition en produit de facteurs premiers (réminiscence, sans doute !).

S'agissant d'une approche élémentaire, je préfère pour ma part l'ordre qui s'appuie sur la division euclidienne (comme celui de mon cours de licence) pour plein de raisons :
1) La démonstration de l'existence de la division euclidienne est facile avec le "bon ordre".
2) C'est quelque chose qui est connu depuis l'école primaire.
3) C'est la propriété la plus forte sur le plan des maths (car euclidien implique principal implique factoriel, aucune des réciproques n'étant vraie)
4) Ça donne un algorithme très simple de calcul du *pgcd* et des coefficients de Bézout.
Bien sûr, par rapport à mon cours, le passage par les congruences n'est pas obligatoire et il peut être omis dans la perspective d'un cours élémentaire. Le seul inconvénient c'est le passage par Bézout qui reste un point difficile. Par rapport à l'ordre que tu proposes, et qui a l'intérêt d'éviter Bézout, j'ai toutefois une réticence forte à admettre le résultat de la proposition 1 car c'est en fait le cœur de l'arithmétique, essentiellement l'unicité de la décomposition en facteurs premiers, bien plus essentielle que l'existence. D'ailleurs, sans ce fait on ne peut pas montrer Gauss par la méthode usuelle et on est très démuni. Mais avec la petite démonstration ci-dessus c'est faisable, non ?