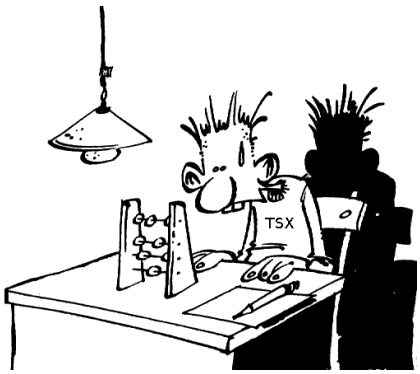
PREMIÈRE LEÇON

ARITHMÉTIQUE I

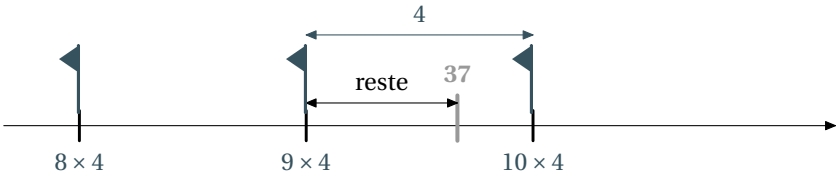


I - EN GUISE D'ÉCHAUFFEMENT...

a. Savez-vous diviser ?

Divisons en dessinant

Vous vous souvenez à peu près du mécanisme de la division que vous avez appris à l'école primaire : vous savez comment ça marche, mais savez-vous pourquoi ça marche ?
Pour vous raffraichir la mémoire, posez la division de 37 par 4.
Pour y voir plus clair, nous « dessiner » cette division. L'idée de base vient du dessin suivant[a] :



Commentez ce schéma.
Puisque nous voulons voir ce qui se passe « après la virgule », nous allons dessiner un segment de droite de 20 cm de long, la première graduation correspondra à 36, la dernière 40, l'unité valant 5 cm.
Placez-y 37.
Divisez alors le segment [36 ; 37] en 10. Que peut-on en déduire ?
Divisez à nouveau en 10 le petit segment contenant 37. Si votre dessin est précis, que remarque-vous ? Qu'en concluez-vous ?

Traduction du dessin en calcul

Si vous tapez [3] [7] [÷] [4] sur votre calculatrice, vous obtenez 9,25 sur votre écran[b].
En pensant aux subdivisions que vous avez tracé sur votre schéma, essayez de traduire le résultat lu à l'aide d'une égalité faisant intervenir 4, $\frac{4}{10}$ et $\frac{4}{100}$.

« J'abaisse un zéro, je mets une virgule »

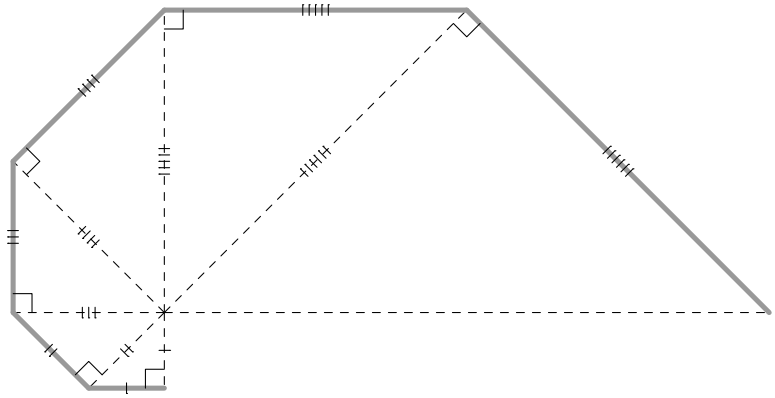
Sans « abaisser de zéro », essayez de reposer votre division en utilisant les phrases « en truc combien de fois quatre », « en truc combien de fois quatre dixièmes », « en truc combien de fois quatre centièmes ».

b. Dessinons des racines

Il aurait été plus correct d'intituler cette activité : **construisons des irrationnels à la règle et à l'équerre**.
Quelle est la longueur de la diagonale d'un carré de côté 1 ? Déduisez-en une *construction* de $\sqrt{2}$.
Construisez de même $\sqrt{5}$, $\sqrt{13}$, $\sqrt{11}$.

Casse-tête en forme d'escargot adepte du cubisme : quelle est la longueur du dixième segment gris de cette spirale[c] ?

[a] C'est même le principe de la démonstration de l'existence de la division euclidienne que nous verrons plus tard.
[b] C'est ce que vous aviez déjà obtenu en posant l'opération...
[c] Je ne vous demande pas de prouver le résultat mais juste de le deviner



c. $\sqrt{2}$ est irrationnel

Qui se cache derrière l'écriture $\sqrt{2}$?

$\sqrt{2}$: qu'est-ce que ça veut dire ? Vous rappelez-vous de la définition vue en collège[d] ?
Pour les grecs, un nombre « existait » si l'on pouvait le dessiner. Ayant à votre disposition une règle de longueur 1 et une équerre, pouvez-vous dessiner $\sqrt{2}$?

Rationnel or not rationnel ?

Comme son nom l'indique, un irrationnel est un nombre qui n'est pas rationnel...
Il serait donc utile de se souvenir de ce qu'est un rationnel : rappelez la définition.
Ainsi, on ne sait pas vraiment ce qu'est un irrationnel, mais on sait ce qu'il n'est pas[e].
Une des premières questions qui surgit de votre esprit en ébullition est sûrement : est-ce que de tels nombres existent ?
Tapons [SHIFT] [$\sqrt{\ }$] [2] sur notre machine. Nous obtenons 1,4142135623731. On pourrait penser qu'en découpant le segment [1 ; 2] en fractions suffisamment petites, on puisse « tomber » sur ce nombre, et donc l'exprimer en fractions d'unité. Que pourrait-on en déduire ?
Supposons donc que $\sqrt{2}$ soit un rationnel. Puisque je connais ma définition, je sais alors qu'il existe deux entiers - appelons-les p et q - tels que $\sqrt{2} = p/q$. Supposons que p et q sont choisis pour que la fraction soit la plus « simple » possible : comment comprenez-vous cette formulation ?

Où nous allons mettre au point un théorème sur la parité

Avant d'aller plus loin, faisons un petit aparté : comment traduire qu'un entier est pair ? Et tant qu'on y est qu'un entier est impair ? Essayer de donner une définition la plus générale possible mais qui permette de caluler[f].
À votre avis, p et q peuvent-ils être tous les deux pairs ?
Observez maintenant les liens entre la parité d'un nombre et celle de son carré sur quelques exemples. Cela vous donne des idées ? Essayez alors d'énoncer un théorème... puis de le prouver !

Revenons à nos moutons

Bon. On suppose donc que $\sqrt{2}$ s'écrit sous la forme p/q, avec p et q les plus simples possibles. Pouvez-vous en déduire des choses sur la parité de p^2 puis sur celle de p ?
Comment peut alors s'écrire p ? p^2 ? q^2 ? Qu'en déduisez-vous sur la parité de q ?
Méditez sur ce résultat.

Considérations sur le raisonnement que nous venons d'utiliser

Otto SCHZPRWT, chef des services secrets syldaves, interroge un homme que des agents des forces spéciales ont surpris en train de rôder autour d'une usine ultra-secrète d'aspirateurs. Pour prouver son innocence, il lui demande de réciter l'hymne à la gloire du Président syldave, mais le prévenu en est incapable. Otto SCHZPRWT en déduit donc qu'il n'est pas un patriote syldave, mais un vil espion à la solde de la Bordurie et le condamne à avaler en moins de 10 minutes une quenelle de grande taille de 18 kg.

[d] Vous pouvez rechercher comment nos voisins européens appellent ce nombre et comment on a pu l'appeler depuis l'Antiquité
[e] C'est clair !
[f] if you see what I mean...

Arrivé à ce moment du récit, vous vous demandez si votre pauvre prof de maths à abusé de la Slivoviz, célèbre eau de vie syldave.
Et bien non ! Car le bon Otto vient d'utiliser le même raisonnement qui nous a conduit à conclure que $\sqrt{2}$ n'était pas rationnel.
Reprenons les faits : notre hypothèse de départ était que $\sqrt{2}$ était rationnel. Après une série de déductions logiques, nous sommes arrivés à une conclusion *absurde*, à savoir que p et q devaient être tous deux pairs.
Par un raisonnement juste, nous sommes arrivés à un résultat faux : c'est donc que notre hypothèse de départ était fausse.
Nous avons effectué un **raisonnement par l'absurde**, qui, malgré son nom, est un type de raisonnement extrêmement rigoureux et que nous utiliserons souvent.
Son utilisation dépasse le cadre mathématique : il est utilisé par les chefs de services secrets mais aussi couramment par les garagistes, les plombiers, les médecins, les détectives privés, etc.
Nous venons de nous initier à la Logique, qui est une discipline qui occupe les esprits depuis des siècles mais qui a connu un véritable essor surtout à partir du début du XX$^{\text{ème}}$ sous l'imulsion du britannique B. RUSSEL.

d. Développement décimal illimité

Curiosité

Observez ce qu'affiche une calculatrice quand vous effectuez les calculs suivants :

$$\frac{324-32}{9} \qquad \frac{3245-32}{99} \qquad \frac{324510-32}{9999}$$

Sans preuve, essayez d'écrire $57,333333333333333333\ldots$ sous forme de fraction.

Une histoire de ...

Par convention, les ... veulent dire qu'il y a une infinité de 3 à droite de la virgule. C'est un peu vague, nous en reparlerons plus bas.
À votre avis, que vaut $1,333\ldots - 1,333$? $1,333 - 1,333$? $1,333\cdots - 1,33$?
Tout ça reste un peu empirique.

L'algèbre au secours de la numération

Nous aimerions prouver ce que nous avons observé tout à l'heure. Essayons donc d'écrire $32,444\ldots$ sous forme de fraction, puisque la machine nous dit que *ça a l'air* possible.
Comme c'est embêtant d'écrire $32,444\ldots$, nous allons lui donner un petit surnom, par exemple *Joe*.
Donc $Joe = 32,444\ldots$.
LA ruse : que vaut $10 \times Joe - Joe$? Déduisez-en que *Joe* est un nombre rationnel puis retrouvez les résultats précédents.

On n'est pas des Mickey

Contrairement à cette charmante souris, nous avons dix doigts et pas huit. Nous comptons donc en **base dix** : qu'est-ce que ça veut dire ?
Pour vous aider à avoir des idées, pensez à ce qui se passe après 9, 99, 999, etc. et surtout, pensez **puissances de 10**.

Trinité

Après des vacances près de Carnac, Plexigladz, le Grand Chef de Gare du peuple syldave[g] a eu une illumination : tout doit marcher par trois. Il a donc ordonné d'effacer de Syldavie tous les chiffres sauf 0, 1 et 2.
Les Syldaves vont donc devoir apprendre à compter en base 3.

En vous inspirant de ce que nous avons dit au sujet de la base dix, essayez de nommer cet objet : 
Plexigladz aime compter ses usines la nuit pour s'endormir : combien en a-t-il[h] ?

[g] C'est à dire le président de Syldavie
[h] en base trois, bien sûr

Développement décimal périodique

Posez la division de 1 par 3, vous obtenez sans cesse le reste 1 et le déloppement décimal est donc 0,33333333333…
En fait, il existe une écriture qui évite les … : $0,\underline{3}$ signifie de la même manière que le 3 se répète infiniment.
Voyez ce que donne 13/7.

```
1 3                  | 7
  6 0                | 1.8 5 7 1 4 2 8 5 7
    4 0              |
      5 0            |
        1 0          |
          3 0        |
            2 0      |
              6 0    |
                4 0  |
                  5 0|
                    1|
```

Donc on écrit $13 \div 7 = 1.\underline{857142}\ldots$

Si, et seulement si

Si je nage en maillot de bain dans un lac syldave **alors** je serai mouillé, mais est-ce que **si** je suis mouillé **alors** je nage en maillot de bain dans un lac syldave ?
La première proposition[i] est une **implication** vraie : nager en maillot de bain dans un lac syldave implique d'être mouillé.
On utilise le symbole $\Longrightarrow$ pour matérialiser cette implication :

$$\text{Nager en maillot dans un lac syldave} \Rightarrow \text{être mouillé}$$

La deuxième proposition[j] est l'**implication réciproque**. Dans le cas qui nous occupe, cette implication réciproque est fausse

$$\text{être mouillé} \not\Rightarrow \text{nager en maillot dans un lac syldave}$$

On dit que ces deux propositions ne sont pas **équivalentes** :

$$\text{Nager en maillot dans un lac syldave} \not\Leftrightarrow \text{être mouillé}$$

Revenons à nos nombres.
En pensant à la division posée, expliquez pourquoi un nombre rationnel admet forcément un développement décimal périodique.
Inversement, expliquez pourquoi un nombre admettant un développement rationnel périodique est forcément rationnel.
Comment exprimer ces résultats en termes d'équivalence ?

$\sqrt{2}$ admet-il un développement décimal périodique ?

Si vous répondez correctement à cette question, alors vous commencerez à vous débrouiller en logique :-)

Les limites du développement décimal

Écrivez sous forme de fraction le nombre $1,\underline{9}$.
Des remarques ?

II - SAVEZ-VOUS COMPTER SUR VOS DOIGTS ?

a. Qu'est-ce qu'un entier ?

Téhessin : C'est une blague ce chapitre ?

Mathémator : Ne vous emballez pas mon petit Téhessin. Je suis persuadé que vous savez compter sur vos doigts, tout comme je suis persuadé que vous obtiendrez bientôt votre permis de conduire une 309 custom, mais savez-vous comment est fabriqué

[i] **Si** je nage en maillot de bain dans un lac syldave **alors** je serai mouillé
[j] **Si** je suis mouillé **alors** je nage en maillot de bain dans un lac syldave

votre carburateur ? vos freins ABS ? Même si vous l'ignorez, vous pourrez décoller à pleine vitesse sur les ralentisseurs de la rue du château. C'est un peu la même chose avec ces entiers si familiers et qui pourtant cachent tant de complexité. On les utilise depuis des millénaires, mais il a fallu attendre les travaux de l'italien Peano à la fin du XIX$^{\text{ème}}$ siècle pour en avoir une présentation $axiomatique$, c'est à dire qu'à partir d'un petit point de départ posé a priori - l'axiome -, on déduit logiquement tout un ensemble de résultats - théorèmes -.

Comment on a fabriqué l'ensemble $\mathbb{N}$
Tout a commencé par quelques axiomes...

1. Il existe une application $s : \mathbb{N} \to \mathbb{N}$, appelée $succession$. L'image d'un entier n par s est appelé $successeur$ de n.
2. Il existe un élément de $\mathbb{N}$ noté 0 qui n'a pas d'antécédent par s (il n'est le successeur de personne). On note 1 le successeur de 0, 2 celui de 1, etc.
3. Chaque entier n admet un unique successeur $s(n)$ et chaque entier non nul est le successeur d'un unique entier.
4. *Axiome de récurrence*
   Si une partie A de $\mathbb{N}$ contient 0 et le successeur de chacun de ses éléments, alors A est en fait égale à $\mathbb{N}$ tout entier.

On peut alors retrouver tout ce qu'on sait sur $\mathbb{N}$ et même plus. On peut par exemple définir une addition + : pour tout couple d'entiers (m,n), $m+0=m$ et $m+s(n)=s(m+n)$. L'axiome de récurrence nous permet de vérifier que cette addition est définie pour tout couple d'entiers et donc que cette définition en est bien une. On obtient ainsi que $s(n)=n+1$

Ce petit aparté présenté pour votre culture générale a néanmoins l'avantage d'introduire un raisonnement clé de notre année de formation :

b. Raisonnement par récurrence

Génétique syldave

Les scientifiques syldaves viennent de mettre en évidence que la terrible maladie de Mathieu est en fait héréditaire : cette maladie frappe depuis des siècles les petits syldaves et les fait naître avec un unique mais énorme cheveu sur la tête.
C'est Vaclav GRTSCHTSZ qui, le premier, contracta cette maladie en 1643 après être rentré en contact avec des vénusiens : ce fait peu connu marque la cause de l'apparition de la maladie en Syldavie. Depuis, tous ses descendants ont souffert de ce terrible mal et aucun médicament terrestre ne semble en mesure de stopper cette calamité.
Résumons les faits :

1. la maladie de Mathieu fait naître les nouveaux nés avec un énorme et unique cheveu sur la tête. Notons n la $n^{\text{ème}}$ génération aprés Vaclav.
   Notons $\mathscr{P}(n)$ la propriété : « la $n^{\text{ème}}$ génération sera infectée par la maldie »
2. initialisation : un premier syldavien est infecté en 1643, donc $\mathscr{P}(0)$ est vraie ;
3. l'hérédité de la maladie a été prouvée : si un des parents de la $k^{\text{ème}}$ génération est atteint, alors ses enfants de la $k+1^{\text{ème}}$ génération seront également infectés, ce qui se traduit par
$$\mathscr{P}(k) \text{ vraie} \Longrightarrow \mathscr{P}(k+1) \text{ vraie}$$
4. nous en déduisons que, quelque soit la génération n des descendants de Vaclav, ceux-ci seront infectés, c'est à dire que $\mathscr{P}(n)$ est vraie quelque soit l'entier naturel n.

Jouons aux cubes

Voici un test de fin d'étude maternelle en Syldavie : prenez un cube, placez en-dessous deux autres cubes, et encore en-dessous trois cubes, etc.

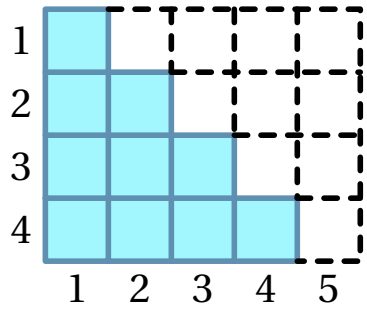


FIG. 1 –

Combien y a-t-il de cubes bleus au total sur le dessin ci-dessus ? On peut encore les compter à la main, mais que faire si je vous demande le nombre de cubes lorsqu'on a placé 100 rangées ? n rangées ?
Le dessin nous donne une idée : si nous complétons la figure pour former un rectangle, il y a deux fois plus de cubes, mais maintenant nous pouvons les compter. Il y en a en effet $\frac{4\times(4+1)}{2}$, et donc

$$1+2+3+4=\frac{4\times(4+1)}{2}$$

Reprenons la méthode adoptée pour étudier la génétique syldave :

1. Nous allons essayer de prouver que la propriété suivante est vraie pour tout entier naturel non nul n

$$\mathscr{P}(n)\ :\ \text{« } 1+2+3+\cdots+n=\frac{n(n+1)}{2}\text{ »}$$

2. Il est facile de vérifier que $1=\frac{1(1+1)}{2}$, donc la deuxième étape de notre raisonnement est vérifiée

$$\mathscr{P}(1)\ \text{ est vraie}$$

3. Supposons qu'une « génération », appelons-la par exemple la $k^{\text{ème}}$, soit « infectée ». Plus sobrement on dira : soit k un entier supérieur à 1. Supposons que $\mathscr{P}(k)$ soit vraie et essayons alors de montrer que cela implique que la génération suivante, la $k+1^{\text{ème}}$, sera elle aussi infectée, c'est à dire

$$\mathscr{P}(k)\ \text{ vraie} \Longrightarrow \mathscr{P}(k+1)\ \text{ vraie}$$

Il s'agit donc de calculer $1+2+3+\cdots+k+(k+1)$ sachant que $1+2+3+\cdots+k=\frac{k(k+1)}{2}$, or

$$\begin{aligned}
1+2+3+\cdots+k+(k+1) &= \underbrace{1+2+3+\cdots+k}\ +(k+1)\\
&= \frac{k(k+1)}{2}\ +(k+1)\\
&= (k+1)\left(\frac{k}{2}+1\right)\\
&= (k+1)\left(\frac{k+2}{2}\right)\\
&= \frac{(k+1)(k+1+1)}{2}
\end{aligned}$$

Nous en déduisons que $\mathscr{P}(k+1)$ est vraie elle aussi.

4. Nous avons vérifié que la propriété était vraie au rang 1 et qu'elle était héréditaire. Nous allons donc en déduire que la propriété sera toujours vraie, quelque soit l'entier naturel non nul n grâce au théorème admis suivant

c. Le théorème

Théorème 1 (admis) Raisonnement par récurrence

Soit $\mathscr{P}$ une propriété dépendant d'un rang n. Pour montrer que $\mathscr{P}(n)$ est vraie pour tous les entiers naturels n supérieurs à un certan n_0

1. On expose clairement la propriété $\mathscr{P}(n)$.
2. On vérifie que $\mathscr{P}(n_0)$ est vraie : c'est le **pas initial** de la récurrence.
3. On **suppose** ensuite que $\mathscr{P}(k)$ est vraie pour un certain entier k : c'est **l'hypothèse de récurrence** et on démontre alors que la propriété $\mathscr{P}(k+1)$ est vraie : c'est le passage du rang k au rang $k+1$ qui exprime que la propriété $\mathscr{P}$ est **héréditaire**.
4. Il reste à **conclure** en annonçant que, par récurrence, la propriété est vraie pour tout entier naturel n

d. Applications

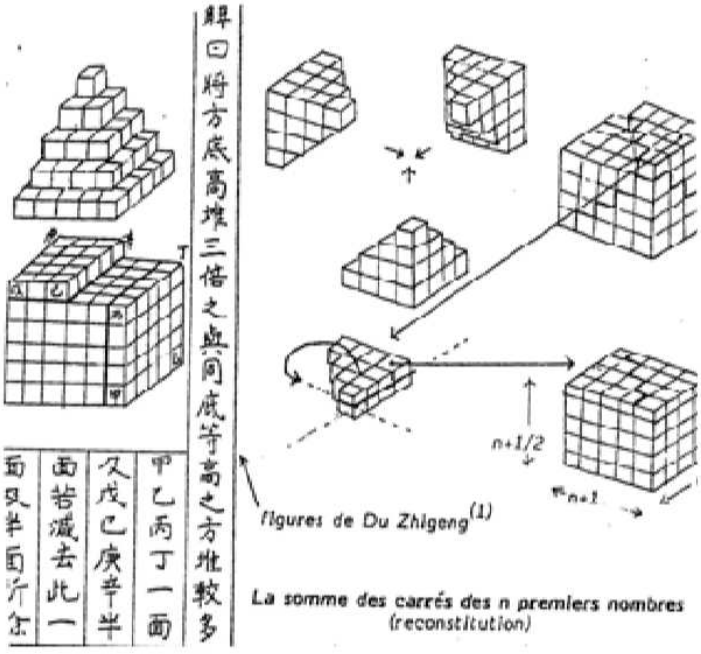
Exercice 1 Jouons encore...

Prenons un cube, rajoutons trois autres cubes pour former un carré, puis cinq autres cubes pour former un plus grand carré, puis sept autres cubes pour former un carré encore plus grand...

Nous voulons maintenant calculer la somme des n premiers entiers impairs.

1. Proposez une formule générale inspirée du résultat de notre petite activité de *maternelle*.
2. Démontrez la formule par récurrence.

Exercice 2 Récurrence chinoise

Que vous inspire le petit dessin suivant (il est interdit de répondre : « rien ! ») 

Et maintenant, avec tout ça on peut définir une multiplication $\times$, une relation d'ordre $\leqslant$[k], une exponentiation[l], une soustraction. Le bonheur quoi. Tout ça pour en arriver à la ...

e. Propriété fondamentale de $\mathbb{N}$

Propriété1

Toute partie non vide de $\mathbb{N}$ possède un plus petit élément

Téhessin : Je ne vois pas trop où est le scoop : c'est sûr que si on prend un groupe de nombre, il y en a forcément un de plus petit.

Mathémator : Eh, eh...Considérez l'intervalle de $\mathbb{R}$ $]32;92]$: quel est son plus petit élément ?

Téhessin : Ben 32.

Mathémator : Sauf que le crochet gauche est ouvert : 32 n'appartient pas à l'intervalle donc ne peut pas être son plus petit élément.

Téhessin : Bon ben 32,1 alors.

Mathémator : Et pourquoi pas 32,0001 ou même 32,00000000000000000001 : vous pouvez comprendre qu'on ne pourra pas trouver de plus petit élément, donc cette propriété n'est pas si bête et va souvent nous servir.

III - DIVISIBILITÉ, MULTIPLES, DIVISEURS

Mathémator : Les mathématiques aiment souvent la symétrie : à chaque entier naturel, on a donc associé un *symétrique* tel que la somme des deux fasse zéro[m] et c'est comme ça qu'on a crée $\mathbb{Z}$. Ensuite, on s'est amusé à multiplier ces entiers entre eux et on a regardé ce qui se passe : c'est l'objet de notre cours d'arithmétique.

Téhessin : Vous voulez me faire croire qu'il suffit de connaître ses tables de multiplication pour assurer en spé math...

Mathémator : À peu de choses près. Par exemple, vous êtes au courant que 45 est un *multiple* de 3, donc que 45 est $divisible$ par 3 ou encore que 3 $divise$ 45. Les petites définitions qui suivent ne vont donc pas vous faire peur :

Définition 1

Soit m et n deux entiers.
Dire que n **divise** m signifie qu'il existe un entier k tel que $m = kn$. On note $n|m$.
On dit alors que n est un **diviseur** de m, que m est un **multiple** de n ou encore que m est **divisible** par n.

Par exemple, on caractérisera un multiple de 3 en disant qu'il s'écrit sous la forme $3k$, avec k un entier.
Comment caractériseriez-vous un entier pair ?

Téhessin : Un entier pair est un multiple de 2, donc il est de la forme $2k$, avec k un entier.

Mathémator : De la même manière, un entier impair est un entier qui n'est pas pair. C'est donc un entier coincé entre deux nombres pairs : c'est le successeur ou le prédécesseur d'un nombre pair.

Téhessin : Donc on peut l'écrire sous la forme $2k+1$ ou $2k-1$: j'assure, non ?

Mathémator : Alors occupez-vous de démontrer les propriétés suivantes :

Propriétés 2

Soit a, b et c des entiers non nuls.

1. Si a divise b et b divise c, alors a divise c.
2. Si a divise b, alors $|a| \leqslant |b|$.
3. Si c divise a et b, alors c divise toute combinaison linéaire à coefficients entiers u et v du type $au+bv$.

[k] Pour les curieux, elle est définie par $m \leqslant n \iff$ il existe $p \in \mathbb{N}$ tel que $m+p=n$
[l] Les puissances quoi
[m] Derrière tout ça se cache la notion de groupe que nous reverrons au moment d'étudier les similitudes

Un petit commentaire sur la troisième propriété : comme 3 divise 6 et 15, alors 3 divise $2\times 6-7\times 15$.
Ensuite, une fois que vous aurez démontré le lemme suivant :

Propriété3
Toute partie majorée de $\mathbb{N}$ est finie et admet un plus grand élément

vous aurez tout le loisir de démontrer

Propriété4
Tout entier non nul admet un nombre fini de diviseurs

IV - DIVISION EUCLIDIENNE

a. Le théorème

Téhessin : Après la maternelle, on passe au CM1 ?

Mathémator : Donc nous progressons...Revenez quelques années en arrière. La maîtresse vous demande de diviser 32 par 5 : que faîtes-vous ?

Téhessin : Je me dis : « en 32, combien de fois 5 ? »

Mathémator : Vous cherchez donc à encadrer 32 par deux multiples consécutifs de 5

Téhessin : Et je conclue par : « il y va six fois et il reste 2 ».

Mathémator : Donc on a $32=6\times 5+2$, mais on aurait pu écrire aussi que $32=4\times 5+12$.

Téhessin : Ah non ! Je vous ai dit qu'il y allait six fois, pas quatre.

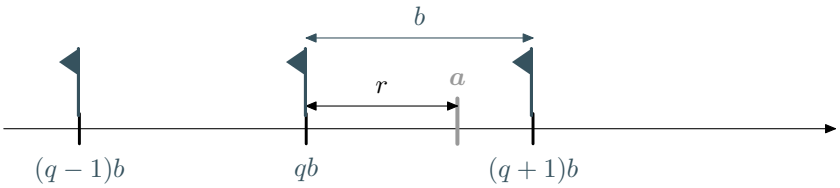
Mathémator : Eh oui : le $reste$ proposé doit être inférieur au $quotient$ 5 pour être sûr d'être entre deux multiples consécutifs de 5.
On peut « résumer » cette idée par le théorème suivant :

Théorème 2
Soit a un entier relatif et b un entier naturel non nul (pourquoi ?).
Il existe un unique couple d'entiers (q,r) tels que

$$a=bq+r \quad \text{avec} \quad 0\leqslant r<b$$

Déterminer q et r, c'est effectuer la division euclidienne de a par b.
On appelle a le dividende, b le diviseur, q le quotient et r le reste.

Qui dit théorème dit démonstration. Le principe de celle qui va suivre est le schéma suivant



qui traduit qu'un entier a est soit un multiple de b, soit est encadré par deux multiples consécutifs de b.
L'énoncé contient deux termes importants : « il $existe$ un $unique$ couple ». Il va donc falloir prouver deux choses :
- qu'un tel couple existe
- qu'il est unique.

Traitons d'abord le cas particulier où $a\in\mathbb{N}$.

Existence Le monde des multiples de b se sépare en deux catégories : ceux qui sont inférieurs (ou égaux) à a et les autres.
En d'autres termes, appelons $\mathscr{M}_i$ l'ensemble des multiples de b inférieurs ou égaux à a. Cet ensemble $\mathscr{M}_i$ est non vide car il contient au moins 0. De plus $\mathscr{M}_i$ est majoré par a puisqu'on l'a défini comme ça.
L'ensemble $\mathscr{M}_i$ est donc une partie de $\mathbb{N}$ non vide et majorée : $\mathscr{M}_i$ admet donc un plus grand élément d'après une propriété que vous avez démontrée.
Appelons μ ce plus grand élément. C'est un multiple de b, donc il existe un entier q tel que $\mu = qb$.
Le multiple suivant est $\mu + b = qb + b = (q+1)b$ qui n'appartient pas à $\mathscr{M}_i$ car il est strictement supérieur au maximum μ.
On en déduit que

$$bq \leqslant a < bq + b$$

C'est ce que nous « montrait » le dessin. Il nous indique aussi que le reste correspond en fait à la différence $a - bq$.
Posons donc $r = a - bq$: on a alors $a = bq + r$ et donc $bq \leqslant bq + r < bq + b$, c'est à dire $0 \leqslant r < b$
Nous avons donc démontré l'existence de deux entiers q et r tels que $a = bq + r$ avec $0 \leqslant r < b$, *inspirés* que nous étions par un joli dessin.
Il reste à démontrer l'unicité d'un tel couple d'entiers.

unicité Une méthode habituelle pour démontrer une unicité est $supposer$ l'existence d'un second couple.
Supposons donc qu'il existe deux couples d'entiers (b, q) et (b', q') vérifiant

$$a = bq + r \quad \text{avec} \quad 0 \leqslant r < b$$
$$a = bq' + r' \quad \text{avec} \quad 0 \leqslant r' < b$$

Effectuons la différence membre à membre de ces égalités. On obtient

$$0 = b(q - q') + r - r' \quad \text{avec} \quad -b < r - r' < b$$

Vous en déduisez comme moi que $r - r'$ est un multiple de b, et que ce multiple est strictement compris entre $-b$ et b.
Le seul multiple qui convient est 0, donc $r - r' = 0$ et par suite $q - q' = 0$, c'est à dire que $r = r'$ et $q = q'$. Dès lors il n'existe qu'un seul couple solution.

Téhessin : Ça c'est de la démonstration ! Mais pourquoi dit-on qu'on ne peut pas diviser par zéro ? Je ne crois pas avoir rencontré de déduction utilisant le fait que b est non nul.

Mathémator : C'est que cela s'est passé vers la fin : vous deviez être épuisé mentalement.
Je vous propose donc un petit jeu : vous répondez à votre propre question et vous traitez le cas où a est strictement négatif connaissant bien sûr le résultat pour $a \in \mathbb{N}$.

Téhessin (à part) : *Voilà un gars qui sait s'amuser.*

b. Notre premier algorithme XCAS

Nous voudrions fabriquer « à la main » un algorithme donnant le quotient et le reste de la division euclidienne de a par b. La preuve du théorème, comme souvent, peut nous donner des idées : en effet, il s'agit de coincer a entre deux multiples consécutifs de b. Par commodité, nous considèrerons que a et b sont des entiers naturels.
On sent qu'un test « tant que » peut s'avérer utile : tant que le multiple de b est inférieur à a, on prend le suivant. Cela donne pour le quotient :

```
quotient(a,b):={
local k;
while(k*b<=a){k:=k+1;}
k-1;
}
}
```

et pour le reste

```
reste(a,b):={
local k;
while(k*b<=a){k:=k+1;}
a-b*(k-1);
}
}
```

Sachez tout de même que ces fonctions sontt pré-programmées de manière plus efficace sur XCAS

```
iquo(2354,67);
irem(2354,67);
```

V - UNE PREMIÈRE SÉRIE D'EXERCICES

a. Divisibilité

Exercice 3

Soit a et b deux entiers.

1. Montrez que pour tout entier naturel non nul, $a-b$ divise a^n-b^n.

Pour l'hérédité, écrivez l'hypothèse de récurrence sous la forme $a^k = bq + (a-b)d$

2. Montrez que pour tout entier naturel $impair$, $a+b$ divise a^n+b^n.

Une récurrence pourrait s'avérer utile en attendant le binôme de Newton. Inspirez-vous de la récurrence précédente.

Exercice 4 VRAI OU FAUX ?

1. Si d divise $a+b$, alors d divise a et b.
2. Si d divise $2a$, alors d divise a.
3. Si d divise a ou b, alors d divise ab.
4. Si d divise ab, alors d divise a ou b.
5. Le produit de deux entiers naturels pairs est pair.
6. La somme de deux entiers naturels pairs est paire.
7. Le produit de deux entiers naturels impairs est impair.
8. La somme de deux entiers naturels impairs est impaire.
9. Le produit d'un entier pair et d'un entier impair est pair.
10. Le produit et la différence de deux entiers relatifs ont toujours la même parité.
11. Le produit de deux entiers consécutifs est pair.
12. La somme de deux entiers impairs consécutifs est divisible par 4.
13. La somme de k entiers consécutifs est divisible par k, avec $k \in [\![2,+\infty[\![$
14. Le produit de k entiers consécutifs est divisible par k, avec $k \in \mathbb{N}^*$
15. $1251^{2p+1}+26^{2p+1}$ est divisible par 1277 pour tout $p \in \mathbb{N}$.
16. $4^{13127}+1$ est un entier naturel qui se termine par 5.

Exercice 5

Prouvez que les entiers suivants sont des multiples de 37 :

1. les nombres de trois chiffres identiques (111, 222, 333,...)
2. les nombres de six chiffres identiques (111 111, 222 222, 333 333,...)
3. les nombres de six chiffres écrits en alternant deux mêmes chiffres (121 212,...)

Exercice 6

1. Soit x un réel différent de 1 et n un entier naturel. Calulez $S_n = \sum_{k=0}^{n-1} x^k$ et retrouvez que $a-b$ divise $a^n - b^n$.

2. Soit $n \in \mathbb{N}^*$ et d un diviseur positif de n.
Montrez que, pour tout entier $a \geqslant 1$, $a^n - 1$ est divisible par $a^d - 1$.

Posez par exemple $n = kd$ et $x = a^p$

3. Montrez que $2^{2004} - 1$ est divisible par 3, 7, 63 et 65.

Exercice 7 Une équation dans $\mathbb{Z}^2$

Résolvez dans $\mathbb{Z} \times \mathbb{Z}$

$$x^2 + 2xy = 15$$

Pensez factorisation et diviseurs de 15

Exercice 8 Relation d'ordre

Relation reflexive On dit qu'une relation $\mathscr{R}$ est reflexive sur un ensemble E si, et seulement si, pour tout élément a de E on a $a \mathscr{R} a$.
Montrez que la relation « divise » est reflexive sur $\mathbb{N}$. Donnez des exemples de relations reflexives et non-reflexives sur des ensembles divers.

Relation transitive On dit qu'une relation $\mathscr{R}$ est transitive sur un ensemble E si, et seulement si, pour tout élément a, b, c de E on a $\begin{cases} a \mathscr{R} b \\ b \mathscr{R} c \end{cases} \Longrightarrow a \mathscr{R} c$.
Montrez que la relation « divise » est transitive sur $\mathbb{N}$. Donnez des exemples de relations transitives et non-transitives sur des ensembles divers.

Relation antisymétrique On dit qu'une relation $\mathscr{R}$ est antisymétrique sur un ensemble E si, et seulement si, pour tout élément a et b de E on a $\begin{cases} a \mathscr{R} b \\ b \mathscr{R} a \end{cases} \Longrightarrow a = b$.
Montrez que la relation « divise » est antisymétrique sur $\mathbb{N}$. L'est-elle sur $\mathbb{Z}$? Donnez d'autres exemples de relations antisymétriques sur des ensembles divers.

Relation d'ordre On dit qu'une relation à la fois reflexive, transitive et antisymétrique sur un ensemble E est une relation d'ordre. Des commentaires ?

VI - CONGRUENCES DANS $\mathbb{Z}$

a. En quoi la division euclidienne nous aide-t-elle à classifier les entiers ?

Mathémator : La section précédente nous a fait découvrir une belle démonstration, mais surtout elle a mis en évidence que, par exemple, le monde des entiers se sépare en trois catégories : les nombres qui s'écrivent sous la forme $3k$, $3k+1$ ou encore $3k+2$, avec k un entier. Ça vous interpelle quelque part ?

Téhessin : Là je sens que vous allez être épaté : quand on divise un nombre par 3, le reste doit vérifier $0 \leqslant r < 3$, donc il ne peut valoir que 0, 1 ou 2. Donc quand on effectue la division euclidienne de n'importe quel entier a, on obtient au choix $a = 3q + 0$ ou $a = 3q + 1$ ou encore $a = 3q + 2$.

Mathémator : Imaginez le mathématicien, assez cossard de nature, devant un tel résultat : il jubile. Au lieu de considérer tous les entiers, ce qui est fastidieux, il va pouvoir se contenter de trois représentants si par exemple leur « position » par rapport à 3 l'intéresse. Ce principe de simplification par l'utilisation de « délégués » est un outil mathématique extrêmement performant qui est le fondement de ce qu'on nomme l'algèbre générale.

Le souci permanent de simplification ne s'arrête pas là : puisqu'on va travailler avec des nombres « délégués », on ne va pas utiliser les règles de calculs des vulgaires nombres du bas-peuple : on va s'inventer un mécanisme de calcul plus performant et élégant. C'est tout l'objet de cette section.

b. Définition et propriétés des congruences

Mathémator : Nous venons de dire que nous allons regrouper les nombres selon leur reste dans la division euclidienne par un entier naturel n quelconque cette fois-ci. Il faut donc définir un code pour se reconnaître entre gens du même monde :

Définition 2

Soient a et b deux entiers et n un entier naturel supérieur à 2.
Dire que a est congru à b modulo n signifie que a et b ont le même reste dans la division euclidienne par n.
On note

$$a \equiv b[n]$$

Téhessin : Mais dites-moi, nous avions déjà rencontré cette notation en trigonométrie. Par exemple $\theta \equiv \frac{\pi}{3}[2\pi]$.

Mathémator : C'est que le problème est similaire : tous les nombres congrus à $\pi/3$ modulo 2π ont un air de famille : ils ont le même représentant sur le cercle trigonométrique. Il n'est donc pas utile de les considérer tous : un « délégué » suffit.
L'atout le plus important des congruences en Terminale, c'est la puissance de calcul qu'elle permettent. Avant d'y venir, faites-vous la main avec cette propriété importante :

Propriété5

Soit a et b deux entiers et n un entier naturel.
a est congru à b modulo n si et seulement si $a-b$ est un multiple de n

Téhessin : Puisque les congruences sont liés au reste, il faut sûrement utiliser les divisions euclidiennes par n.
Je pose donc $a = nq + r$ et $b = nq' + r'$ sans oublier que r et r' sont dans $[\![0, n[\![$.
Comme $a \equiv b[n]$, on a $r = r'$ par définition des congruences.
Alors $a - b = nq + r - nq' - r' = nq - nq' = n(q - q')$ et j'obtiens bien que $a - b$ est un multiple de n.

Mathémator : Pas mal...mais vous n'avez fait que la moitié du boulot : le « si et seulement si » signifie que les assertions sont équivalentes, c'est à dire que
- **si** $a \equiv b[n]$, **alors** $a - b$ est un multiple de n
ET réciproquement
- **si** $a - b$ est un multiple de n, **alors** $a \equiv b[n]$

Téhessin : Autant pour moi. Cette fois-ci, nous supposons que $a - b$ est un multiple de n, donc il existe un entier k tel que $a - b = kn$.
Or $a - b = n(q - q') + r - r'$, donc $r - r' = n(k - q + q')$. Bon, $r - r'$ est donc un multiple de n, mais de là à dire que $r = r'$...

Mathémator : Ah lala lala...si seulement vous étudiez vos démonstrations de cours, cela vous donnerait des idées. Revoyez donc ce que nous avons fait pour prouver l'unicité de la division euclidienne.

Téhessin : Ah c'est sûr, tout s'éclaire : $r - r'$ est un multiple de n qui vérifie $-n < r - r' < n$. Il n'en existe qu'un seul :zéro, donc $r = r'$ et par définition, on obtient bien que $a \equiv b[n]$.

Mathémator : Cette propriété nous permet en fait d'exploiter autrement les congruences. En effet, si par exemple $x \equiv 5[32]$, cela signifie qu'il existe un entier k tel que $x - 5 = 32k$, soit encore que $x = 5 + 32k$.

Propriété6

$$a \equiv b[n] \iff \text{il existe un entier } k \text{ tel que } a = b + kn$$

Téhessin : Ça ressemble à la division euclidienne de a par n.

Mathémator : Mais ça peut ne pas l'être : n'oubliez pas que le reste doit obligatoirement être positif et strictement inférieur au diviseur.
Par exemple on a bien $33 \equiv 97[32]$, mais 97 n'est certes pas le reste de la division de 33 par 32.

Occupez-vous à présent de quelques propriétés extrêmement intéressantes des congruences

Propriétés 7

Comme d'habitude, n est un entier naturel supérieur à 2 et tous les autres sont des entiers relatifs.

1. $a \equiv a[n]$

2. Si $a \equiv b[n]$, alors $b \equiv a[n]$

3. Si $a \equiv b[n]$ et $b \equiv c[n]$, alors $a \equiv c[n]$

4. Si $a \equiv b[n]$ et $a' \equiv b'[n]$, alors

$$a + a' \equiv b + b'\ [n] \quad a - a' \equiv b - b'\ [n] \quad aa' \equiv bb'\ [n]$$

5. Si $a \equiv b[n]$, alors, pour tout $p \in \mathbb{N}$, $a^p \equiv b^p[n]$

En fait, il faut retenir qu'on peut additionner, soustraire, multiplier des congruences **de même module**.

Téhessin : Vous avez oublié la division.

Mathémator : Et pour cause : c'est une opération à haut risque quand on travaille avec des entiers.
Par exemple $12 \equiv 0[6]$, mais $\frac{12}{3} \not\equiv \frac{0}{3}[6]$.
L'utilisation des congruences nous ouvre les portes d'une multitude d'exercices. Elle va également nous permettre de revenir sur les bases de la numération que vous avez découvertes en primaire.

c. Les bases sur les bases

Mathémator : Vous utilisez depuis votre tendre enfance le système de numération décimale. Si nous étions tous des Mickey, nous aurions sûrement préféré compter en base 8. Les ordinateurs, eux, préfèrent compter en base 2 et de plus en plus maintenant en base 16. Cela me rappelle mon jeune temps : j'étais un sage petit Mataïe en classe de CM1 et je jouais aux cubes : quand j'avais 3 cubes, je les remplaçais par une barre de 3, quand j'avais 3 barres je les remplaçais par une plaque, quand j'avais trois plaques je les remplaçais par un cube... ëtes-vous capable de commenter ces délirantes activités qui faisaient de mes journées à l'école un enchantement ?

Téhessin (à part) : *C'est dur de veillir...*

Mathémator : Mais j'ai grandi depuis, alors pour faire plus sérieux je vous propose la propriété suivante

Numération en base b

Soit b un entier supérieur à 2. On peut écrire de manière unique tout entier naturel a sous la forme

$$a = a_n \times b^n + a_{n-1} \times b^{n-1} + \cdots + a_1 \times b^1 + a_0 \quad \text{avec } 0 \leqslant a_i \leqslant b-1 \text{ et } a_n \neq 0$$

On note $a = \overline{a_n a_{n-1} \cdots a_1 a_0}^{\,b}$

Encore une fois, le problème se sépare en deux : existence puis unicité d'une telle écriture. Vous vous en occuperez en exercice. Vous prouverez également certains critères de divisibilité que vous utilisez depuis le primaire.

VII - POUR DIRE LES CHOSES PLUS SIMPLEMENT...

Avant de voir tous vos neurones fondre comme des fusibles 10 ampères dans une centrale atomique, il est temps d'adopter un plan d'urgence. Si les congruences sont quasi inexistantes dans votre livre vieux de quatre ans, elles sont devenues les coqueluches des poseurs de sujet comme vous le constaterez sr le recueil d'exercices de Bac. Je me suis donc replongé dans mon vieux livre de cm1...
Voici un classement des entiers naturels

0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	...			

Vous pouvez aussi enrouler la droite des réels graduée par les entiers sur un cercle de périmètre 5 et retrouver les mêmes sensations qu'avec la congruence modulo 2π : il vous semble assez naturel de penser $\pi/3$, $7\pi/3$, $-5\pi/3$ « représentent » le même réel sur le cercle trigonométrique. Et bien 1, 6, 11, 16, ... représentent le même entier sur le « cercle modulo 5 »

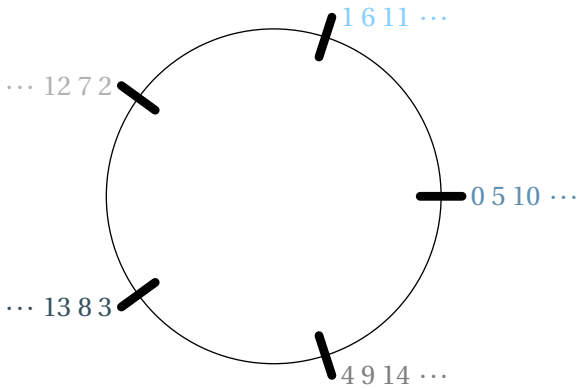


FIG. 2 –

Cela nous permet de classer les entiers par équipes : l'équipe de ceux qui ont pour reste 0 dans la division euclidienne par 5, l'équipe de ceux qui ont pour reste 1, etc.
Maintenant, si Roger, Bébert et Josette font partie de la même équipe, on pourra désigner cette équipe par « équipe de Roger » ou « équipe de Bébert » ou bien « équipe de Josette ».
Pour nos nombres, l'équipe de ceux qui ont pour reste 3 pourra s'appeler l'équipe de 3 ou l'équipe de 8 ou l'équipe de 32318.
Point de vue congruence, cela donne

$$3 \equiv 8[5] \quad 3 \equiv 32318[5] \quad 32318 \equiv 8[5]$$

On souhaite maintenant additionner ces équipes. Il ne s'agit pas de l'addition usuelle des entiers. Par exemple, si on note $\dot{3}$ l'équipe de 3, on obtient

$$\dot{3}\dot{+}\dot{2} = \dot{0} \quad \dot{4}\dot{+}\dot{4} = \dot{3} \quad \dot{4}\dot{+}\dot{4} = \dot{-2}$$

et comme la multiplication des entiers, c'est une suite d'additions, on a également

$$\dot{3}\dot{\times}\dot{2} = \dot{1} \quad \dot{7}\dot{\times}\dot{5} = \dot{0} \quad \dot{3}\dot{\times}\dot{8} = \dot{-1}$$

VIII - DES EXERCICES UTILISANT LES CONGRUENCES.

Exercice 9 Tables d'addition et de multiplication

a) Complétez le tableau en n'utilisant que $\dot{0}$, $\dot{1}$, $\dot{2}$, $\dot{3}$ et $\dot{4}$...

$\dot{+}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$					
$\dot{1}$					
$\dot{2}$					
$\dot{3}$					
$\dot{4}$					

b) ... et pour rigoler, celui-ci aussi

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$					
$\dot{1}$					
$\dot{2}$					
$\dot{3}$					
$\dot{4}$					

Exercice 10

Vous pouvez même résoudre les équations suivantes dans $\mathbb{Z}$

$$1+1\equiv 0[x] \quad 3+x\equiv 2[7] \quad 8+6\equiv 5[x]$$

Exercice 11

Allez, un dernier exercice tiré du livre de cm1

Les nombres 13, 21, 32, 36, 40, 45 et 77 sont écrits en base dix. Si tu voulais les écrire en base trois, quels sont ceux qui auraient pour chiffre des unités 0, 1, 2 ? Quels sont ceux qui auraient pour chiffre des unités 0, 1, 2, 3, 4 si tu voulais les écrire en base cinq ?

On essaie des formulations plus « terminale »

Exercice 12

Soit x et y deux entiers naturels tels que $x\equiv 7[9]$ et $y\equiv 4[9]$. Déterminez les restes dans la division par 9 de

$$a)\ 3x+4y \qquad b)\ x^2+y^2 \qquad c)\ 2x^2-5y^2$$

Exercice 13 Vrai ou Faux ?

1. On suppose que $a\equiv 1[n]$, alors $a^n\equiv 1[n]$

2. On suppose que $a\equiv 3[n]$, alors $a^n\equiv 3[n]$

Exercice 14

Trouvez le reste de la division par 5 du nombre 12^{1527}.

$2^4\equiv 1[5]$ *et* $1527\equiv 3[4]$

Exercice 15

Montrez que, pour tout naturel n,

$$3^{3n+2}+2^{n+4}\equiv 0[5]$$

Exercice 16

Montrez que

$$a)\ 34^{57}\equiv 1[11] \qquad b)\ 328^{42}\equiv 4[5] \qquad c)\ 3\,174^{249}\equiv 2[11]$$

Exercice 17

Pour quelles valeurs de n a-t-on $3^n \equiv 0[2]$

Exercice 18 un exo de bac pour finir sur une note optimiste

1. Montrez que pour tout naturel n, $24n^2+8n$ est divisible par 16.

2. Déduisez-en que $(2n+1)^4 \equiv 1[16]$

3. Montrez que, si $a \in \mathbb{N}$, a^4 est congru à 0 ou 1 modulo 16.

4. Déduisez-en que, si le nombre $16n+15$, avec $n \in \mathbb{N}$, est mis sous la forme d'une somme de k puissances quatrièmes d'entiers, *i.e.* $16n+15 = x_1^4 + x_2^4 + \cdots + x_k^4$, alors nécessairement $k \geqslant 15$

Exercice 19 Relation d'équivalence

On dit qu'une relation $\mathscr{R}$ est **symétrique** sur un ensemble E si et seulement si, pour tout couple (a,b) de E × E

$$a\mathscr{R}b \Longrightarrow b\mathscr{R}a$$

Une relation qui est à la fois reflexive, symétrique et transitive est une **relation d'équivalence** (cf exercice8 page12)
La relation ≡ est-elle une relation d'équivalence ?

Exercice 20

Dans tout l'exercice, on évitera de passer par la base 10.

1. Un entier s'écrit 1.011.111.101.000 en base deux. L'écrire en base huit.

2. Un entier s'écrit 572.634 en base huit. L'écrire en base deux.

Exercice 21 Critères de divisibilité à partir de l'écriture décimale

Justifiez les critères de divisibilité suivants. Les chiffres dont il est question dans les différents critères sont ceux de l'écriture décimale de l'entier naturel n que l'on teste. Si besoin est, on notera ces chiffres $c_{p-1}, \cdots, c_0$ de telle sorte que $n = \overline{c_{p-1}\cdots c_0}^{10}$, et on posera $c_k = 0$ pour $k \geqslant p$.

1. n est divisible par 2 si et seulement si son chiffre des unités c_0 est égal à 0,2,4,6 ou 8.

2. n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

3. n est divisible par 4 si et seulement si le nombre formé par ses deux derniers chiffres (i.e. $\overline{c_1c_0}^{10}$) est lui-même divisible par 4.

4. n est divisible par 5 si et seulement si son chiffre des unités c_0 est égal à 0 ou 5.

5. n est divisible par 7 si et seulement si $\overline{c_2c_1c_0}^{10} - \overline{c_5c_4c_3}^{10} + \overline{c_8c_7c_6}^{10} + \cdots$ est divisible par 7.

6. n est divisible par 8 si et seulement si le nombre formé par ses trois derniers chiffres (i.e. $\overline{c_2c_1c_0}^{10}$) est lui-même divisible par 8.

7. n est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

8. n est divisible par 10 si et seulement si son chiffre des unités c_0 est égal à 0.

9. n est divisible par 11 si et seulement si $c_0 - c_1 + c_2 - c_3 + \cdots$ est divisible par 11.

10. n est divisible par 13 si et seulement si $\overline{c_2c_1c_0}^{10} - \overline{c_5c_4c_3}^{10} + \overline{c_8c_7c_6}^{10} + \cdots$ est divisible par 13.

Exercice 22 Existence et unicité de l'écriture d'un nombre en base b

On rappelle le théorème de cours

Numération en base b

Soit b un entier supérieur à 2. On peut écrire de manière unique tout entier naturel a sous la forme

$$a = a_n \times b^n + a_{n-1} \times b^{n-1} + \cdots + a_1 \times b^1 + a_0 \quad \text{avec } 0 \leqslant a_i \leqslant b-1 \text{ et } a_n \neq 0$$

On note $a = \overline{a_n a_{n-1} \cdots a_1 a_0}^{\,b}$

1. Existence.

a) Justifiez que a peut s'écrire

$$a = bq_0 + a_0, \text{ où } 0 \leqslant a_0 \leqslant b-1 \text{ et } q_0 < a$$

Justifiez que si $q_0 < b$, le problème est résolu.

b) Si $q_0 \geqslant b$, réitérer le procédé.
Justifiez que ce procédé s'arrête au bout d'un nombre fini d'itérations.

2. Démontrez l'unicité de l'écriture.

Exercice 23 Triangle rectangle à côtés entiers.

Les mesures des côtés d'un triangle rectangle sont des nombres entiers a, b et c.

1. Démontrez que l'un au moins des trois nombres est pair.

2. Démontrez que l'un au moins des trois nombres est divisible par 3.

3. Démontrez que l'un au moins des trois nombres est divisible par 4.

4. Démontrez que l'un au moins des trois nombres est divisible par 5.

Exercice 24 Sommes de carrés

1. Montrer qu'un entier congru à 3 modulo 4 n'est pas somme de deux carrés d'entiers.

2. Montrer qu'un entier congru à 7 modulo 8 n'est pas somme de trois carrés d'entiers.

Un peu de culture

Au vu des deux résultats précédents, on pourrait croire qu'un entier congru à 15 modulo 16 n'est pas somme de quatre carrés d'entiers, mais c'est faux... car tout entier naturel est somme de quatre carrés !

Exercice 25

Montrez que, pour tous entiers m et n, $m^2 + n^2$ est divisible par 7 si et seulement si m et n sont divisibles par 7.

Résumez dans un tableau les valeurs que peut prendre k^2 modulo 7, avec k un entier quelconque.

Exercice 26

Résolvez dans $\mathbb{N}^2$ l'équation $2^x - 5^y \equiv 3[24]$.

Montrez par récurrence que 2^n ne prend que deux valeurs modulo 24 à partir d'un certain rang. De même avec 5^n.

Exercice 27

Quel est le chiffre des unités des nombres suivants :

$$a = 2001^{2003^{2005}} \quad b = 2003^{2004^{2005}} \quad c = 2003^{2005^{2004}} \quad d = 2007^{2008^{2009}}$$

Exercice 28 VRAI OU FAUX ?

1. Tout carré est congru à 0 ou 1 modulo 8.

2. Si $(x^2-1)^2$ n'est pas multiple de 4, alors x l'est.

Exercice 29

1. Soit $n \in \mathbb{N}^*$. Montrez que 5 divise $n(n^4-1)$.

2. Déduisez-en que, si $p \in \mathbb{N}^*$, n^p et n^{p+4} ont le même chiffre des unités.

Exercice 30

Le plan est rapporté à un repère orthonormal $\left(O; \vec{u}, \vec{v}\right)$. Existe-t-il des points à coordonnées entières sur le cercle de centre O et de rayon $5\sqrt{27\,723}$?

Quels sont les restes possibles dans la division par 4 d'une somme de deux carrés ?

Exercice 31 $\sqrt{2}$ est irrationnel

Supposons qu'il existe $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$ tels que $\sqrt{2} = a/b$. En étudiant les chiffres des unités de a, a^2, b, $2b^2$, montrez qu'on arrive à une contradiction.

Exercice 32 $\sqrt{2}$ est décidément irrationnel

Le plan est rapporté à un repère $\left(O; \vec{u}, \vec{v}\right)$. On considère la droite D d'équation $y = \sqrt{2}x$ et l'application f qui, à tout point M(x, y) du plan, associe le point M$'(x', y')$ défini par

$$\begin{cases} x' = 3x - 2y \\ y' = -4x + 3y \end{cases}$$

Nous ferons l'hypothèse suivante : « il existe un point m_0 de D dont les coordonnées x_0 et y_0 sont des entiers strictement positifs ».

On considère le point $m_1 = f(m_0)$ de coordonnées (x_1, y_1) puis on réitère le procédé pour obtenir une suite $(m_k)_{k\in\mathbb{N}}$ de points de coordonnées (x_k, y_k).
Montrez que tous les points m_k appartiennent à D et que les suites (x_k) et (y_k) sont des suites strictement décroissantes d'entiers strictement positifs.
Expliquez le choix du titre de cet exercice.

Un peu de culture
Cette méthode de démonstration, dite de *descente infinie*, a été découverte par Fermat au XVII$^{\text{ème}}$ siècle.

.

IX - PGCD

a. Définition

Considérons un entier relatif a. On notera $\mathscr{D}(a)$ l'ensemble de ses diviseurs dans $\mathbb{Z}$.
Par exemple, $\mathscr{D}(0)=\mathbb{Z}$, $\mathscr{D}(1)=\{-1,1\}$, $\mathscr{D}(12)=\{-12,-6,-4,-3,-2,-1,1,2,3,4,6,12\}$ et plus généralement

$$\mathscr{D}(a)=\{-|a|,...,-1,1,...,|a|\}$$

Définition 3 PGCD

Soit a et b deux entiers. On appelle PGCD de a et b et on note $a\wedge b$ l'entier défini de la manière suivante :

- $0\wedge 0=0$
- Si a et b ne sont pas simultanément nuls, $a\wedge b$ est le plus grand entier naturel qui divise simultanément a et b.

Le PGCD de a et b est donc le plus grand élément de $\mathscr{D}(a)\cap\mathscr{D}(b)$: la notation le rappelle. Comme toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément, cette définition en est bien une car $\mathscr{D}(a)\cap\mathscr{D}(b)$ contient au moins 1.

b. Égalité de Bézout

Voici la clé de notre chapitre : nous allons montrer que notre PGCD est en fait une combinaison linéaire de a et de b.
Cette idée est due au français Étienne Bézout(1730 - 1783) dont vous pouvez admirer le charmant portrait.

Considérons d'abord le cas où a et b sont non nuls et notons

$$S=\left\{au+bv \mid (u,v)\in\mathbb{Z}^2 \text{ et } au+bv>0\right\}$$

L'ensemble S est constitué d'entiers naturels et est non vide car il contient au moins a^2+b^2 : il admet donc un unique **plus petit élément** que nous noterons d qui s'écrit donc $d=au_0+bv_0$.
Notre mission va bien sûr consister à prouver que d est en fait le PGCD de a et b.

Nous allons pour cela utiliser une ficelle classique : introduire le reste de la division euclidienne de a par d et utiliser le fait que d est le plus petit élément de S puis raisonner par l'absurde.
La division de a par d s'écrit

$$a=dq+r \quad \text{avec} \quad 0\leqslant r<d$$

Supposons que $r>0$, alors

$$r=a-dq=a-q(au_0+bv_0)=a(1-qu_0)+b(-qv_0)>0$$

et donc $r\in S$ or $r<d$. C'est impossible car d est le plus petit élément de S : **contradiction**.
Notre supposition de départ est donc fausse et $r=0$. Nous en déduisons que d divise a.
On montre de manière similaire que d divise b. Ainsi

$$d \text{ est un diviseur commun de } a \text{ et } b$$

Il nous reste à montrer que c'est le plus grand. Soit δ un diviseur commun à a et b quelconque. On a montré au début du cours (Propriété XX-2) qu'alors δ divisait toute combinaison linéaire de a et de b, donc en particulier δ divise au_0+bv_0 donc d. Alors toujours d'après la propriété XX-2, $c\leqslant|d|=d$, donc d est bien le plus grand des diviseurs.

Il faut encore vérifier que le PGCD est **unique**. La méthode habituelle est de supposer qu'il existe un deuxième PGCD, disons d'. Alors $d\leqslant d'$ car d' est le plus grand diviseur puis $d'\leqslant d$ car d aussi et finalement $d=d'$ ce qui assure l'unicité.

Comme $|a|=\pm1\times a+0\times 0$, l'égalité tient toujours si b (ou a) est nul, donc

Théorème 3 Égalité de Bézout

Soit a et b deux entiers relatifs.
Si $d = a \wedge b$, alors il existe deux entiers u et v tels que

$$au + bv = d$$

Ce résultat est beaucoup plus important qu'il n'y parait. Nous allons d'abord voir quelques conséquences immédiates.

c. Premières propriétés

Soit δ un diviseur commun à a et b. Alors il divise aussi $au+bv$ donc d comme nous l'avons déjà vus. Inversement, un diviseur de d divise aussi a et b, d'où

Propriété8

Les diviseurs communs à a et b sont les diviseurs de leur PGCD

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$$

De plus, $a \wedge b$ divisant toute combinaison linéaire de a et b, donc toute combinaison linéaire de a et b est un multiple de $a \wedge b$. Inversement, puisqu'il existe deux entiers u et v tels que $a \wedge b = au + bv$, on a $k(a \wedge b) = (ku)a + (kv)b$ et donc tout multiple de $a \wedge b$ est une combinaison linéire de a et b

Propriété9

L'ensemble $S = \left\{ax + by \mid (x, y) \in \mathbb{Z}^2\right\}$ constitue l'ensemble de tous les multiples de $d = a \wedge b$, c'est à dire

$$S = d\mathbb{Z}$$

Par exemple, l'équation $15x + 12y = 5$ ne peut pas avoir de solution dans $\mathbb{Z}$ car $15 \wedge 12 = 3$ et 5 n'est pas un multiple de 3.

Donnons maintenant quelques propriétés évidentes

Propriété10

- $a \wedge b = b \wedge a$
- $a \wedge a = a$
- $a \wedge 1 = 1$
- $a \wedge b = b \Longleftrightarrow b|a$

Nous nous restreindront dans la suite à des entiers naturels car

Propriété11

$$a \wedge b = |a| \wedge |b|$$

Voyons maintenant une propriété qui va être à la base de la construction algorithmique du PGCD

Propriété12

Si $ab \neq 0$ et k un entier quelconque

$$a \wedge (b+ka) = a \wedge b$$

et en particulier

$$a \wedge b = a \wedge (b-a) = a \wedge (a-b)$$

La démonstration est classique et nous servira à de nombreuses occasions.
Notons $a \wedge b = d$ et $a \wedge (b+ka) = d'$. Alors

- d divisant a et b, d divise $(ka+b)$ et a donc divise d' d'après une propriété précédente.
- d'autre part, d' divise a et $b+ka$, donc divise $b+ka-ka$, donc b, donc d' est un diviseur commun à a et b donc d' divise d.

Comme $d|d'$ et $d'|d$, on a donc $d = d'$.

Cette propriété va nous permettre de fabriquer un algorithme de calcul de $a \wedge b$. En effet, si $a \geqslant b$, et comme $a \wedge b = b \wedge (a-b)$, on calcule le PGCD de deux entiers plus petits. Et on réitère. Par exemple :

$$15 \wedge 12 = 12 \wedge 3 = 9 \wedge 3 = 6 \wedge 3 = 3 \wedge 3 = 3 \wedge 0 = 3$$

ce qui donne en xcas

```
pgcd1(a,b):={
if (b=0) return a;
if (a>=b) return(pgcd1(b,a-b));
else return(pgcd1(a,b-a));
}
```

Comment se persuader que cette descente aboutit ? Nous pouvons aisément nous convaincre sans se perdre dans trop de formalisme que

Propriété13 Suite décroissante d'entiers naturels

Toute suite strictement décroissante d'entiers naturels est finie.

Et cette constante ne pouvant être par construction que 0, le PGCD de a et b sera la dernière valeur non nulle de cette suite car $k \wedge 0 = k$ pour tout entier k.
Ce procédé semble assez long : beaucoup d'opérations sont inutiles. Malgré tout il est assez efficace car il n'utilise que des sommes et des différences qu'un ordinateur traite extrêmement rapidement.

d. Algorithme d'Euclide

C'est le même principe que ce que nous venons de faire, mais en plus rapide car nous remarquons que, en notant

$$a = bq_0 + r_0 \quad \text{avec } 0 \leqslant r_0 < b$$

la division euclidienne de a par b, on obtient que

$$a \wedge b = b \wedge (a - bq_0) = b \wedge r_0$$

Puis en notant

$$b = r_0 q_1 + r_1 \quad \text{avec } 0 \leqslant r_1 < r_0$$

on obtient de même que

$$a \wedge b = b \wedge r_0 = r_0 \wedge r_1$$

et on continue ainsi à fabriquer une suite strictement décroissante d'entiers naturels : elle est donc finie et son dernier terme $r_p = 0$.
Alors

$$a \wedge b = r_{p-1} \wedge r_p = r_{p-1} \wedge 0 = r_{p-1} = \text{ le dernier reste non nul}$$

Donnons deux algorithmes XCAS donnant le pgcd : l'un itératif, l'autre récursif et utilisant tous deux la fonction irem(a,b) vue précédemment qui donne le reste de la division euclidienne de a par b :

```
pgcd2(a,b):={
local r;
while(b!=0){
r:=irem(a,b);
a:=b;
b:=r;
}
return(a);
}
```

et une version récursive :

```
pgcd3(a,b):={
if (b==0)
return(a);
else
return(pgcd3(b,irem(a,b)));
}
```

Nous pouvons traduire pgcd2 en langage ti89 :

```
:pgcd2(a,b)
:Func
:Local r
:  While b<>0
:    irem(a,b) => r
:    b => a
:    r => b;
:   EndWhile
:  Return a
:EndFunc
```

ou en langage ti<89 :

```
Prompt a
Prompt b
  While b!=0
     a-b*Int(a/b)-> r
    b -> a
    r -> b;
  End
Disp  a
```

ou en langage Casio :

```
"a" : ? -> a
"b" : ? -> b
  While b!=0
     a-b*Int(a/b)-> r
    b -> a
    r -> b;
  WhileEnd
a
```

XCAS a une fonction très éfficace pour calculer les PGCD : `igcd(a,b)`. Pourtant, il est *pédagogiquement* important de voir différents algorithmes de calcul, histoire de n'être pas seulement des consommateurs...

Sans ordinateur, on peut présenter les calculs sous forme de tableau.
Il nous reste un dernier algorithme à découvrir, qui nous donnera des coefficients des égalités de Bézout.

e. Algorithme d'Euclide étendu

L'algorithme d'Euclide nous assure que le PGCD de a et b est le dernier reste non nul de la suite (r_k) construite au paragraphe précédent. L'égalité de Bézout nous assure de l'existence de deux entiers u et v tels que $au+bv = a\wedge b$.
Nous allons essayer de combiner les deux en construisant deux suites (u_k) et (v_k) telles que

$$r_k = au_k + bv_k$$

Voici le départ

- $r_0 = a = 1\times a + 0\times b$
- $r_1 = b = 0\times a + 1\times b$
- $r_2 = \texttt{reste}(r_0, r_1)$

  $\vdots$
- $r_{i+1} = \texttt{reste}(r_{i-1}, r_i)$

  $\vdots$
- $r_{p-1} = a\wedge b$
- $r_p = 0$

Or par définition, comme $r_2 = \texttt{reste}(r_0, r_1)$, on a $r_0 = q_2 r_1 + r_2$, donc $r_2 = 1\times r_0 - q_2 \times r_1$, c'est à dire

$$u_2 = 1 \text{ et } v_2 = -q_2$$

On réitère le mécanisme. Supposons que $r_{k-1} = u_{k-1}\times a + v_{k-1}\times b$ et $r_k = u_k \times a + v_k \times b$
Comme $r_{k+1} = \texttt{reste}(r_k, r_{k-1})$, on a $r_{k-1} = q_{k+1}r_k + r_{k+1}$, donc $r_{k+1} = 1\times r_{k-1} - q_{k+1}\times r_k$, c'est à dire

$$r_{k+1} = 1\times(u_{k-1}\times a + v_{k-1}\times b) - q_{k+1}\times(u_k\times a + v_k \times b)$$

Finalement

$$u_{k+1} = u_{k-1} - u_k \times q_{k+1} \text{ et } v_{k+1} = v_{k-1} - v_k \times q_{k+1}$$

Ça a l'air un peu brut comme ça, au premier coup d'œil, mais en fait il y a une disposition pratique qui permet de mieux voir ce qui se passe. D'abord, dans algorithme d'Euclide étendu il y a algorithme d'Euclide, donc on commence par rechercher le PGCD de a et b par l'algorithme d'Euclide en n'oubliant pas cette fois de noter les quotients en remplissant le tableau suivant

k	u_k	v_k	r_k	q_k
0	1	0	a	/
1	0	1	b	q_1
2			r_2	q_2
3			r_3	q_3
$\vdots$			$\vdots$	$\vdots$
$p-1$			$r_{p-1} = a\wedge b$	q_{p-1}
p			$r_p = 0$	

Et le secret tient dans le schéma

$$\boxed{u_k} \quad - \quad \left(\boxed{u_{k+1}} \times \boxed{q_{k+1}} \right) \quad = \quad \boxed{u_{k+2}}$$

et pareil pour les v_k.
Voyons tout de suite sur un exemple simple : cherchons u et v tels que

$$19u + 15v = 19\wedge 15$$

k	u_k	v_k	r_k	q_k	
0	1	0	19	/	L_0
1	0	1	15	1	L_1
2	1	-1	4	3	$L_2 \leftarrow L_0 - 1 \times L_1$
3	-3	4	3	1	$L_3 \leftarrow L_1 - 3 \times L_2$
4	4	-5	1	3	$L_4 \leftarrow L_2 - 1 \times L_3$
5			0		$L_5 \leftarrow L_3 - 3 \times L_4$
6				0	

Le dernier reste non nul est 1 donc $19 \wedge 15 = 1$ et $4 \times 19 - 5 \times 15 = 1$
On peut naturellement utiliser le tableur XCAS pour obtenir ces résultats. On peut égalment crée des algorithmes ...pour vos calculatrices.

```
bezout(a,b):={
local la,lb,lr,q,lb2;
la:=[1,0,a];
lb:=[0,1,b];
lb2:=b;
while (lb2 !=0){
q:=quotient(la[2],lb2);
lr:=la+(-q)*lb;
la:=lb;
lb:=lr;
lb2:=lb[2];
}
return(la);
}
```

Remarque 0.1 : *Il existe bien sûr une fonction XCAS qui fait ça très vite et très bien :* `igcdex(a,b)` *renvoie les deux coefficients et le PGCD.*

En ti :

```
Input "A=", R
Input "B=", Y
1->U: 0->W: 0->V: 1->X
While Y !=0
Int(R/Y)->Q
U->Z: W->U: Z-Q*W->W
V->Z: X->V: Z-Q*X->X
R->Z: Y->R: Z-Q*Y->Y
End
Disp"U=",U,"V=",V
Disp "PGCD=",R
```

En Casio :

```
"A=" :? -> R
"B=" :? -> Y
1->U: 0->W: 0->V: 1->X
While Y !=0
Int(R/Y)->Q
U->Z: W->U: Z-Q*W->W
V->Z: X->V: Z-Q*X->X
R->Z: Y->R: Z-Q*Y->Y
WhileEnd
"U=":U : "V=":V
"PGCD=" :R
```

f. Petits exercices

Exercice 33

Trouvez tous les diviseurs communs à :

a) 300 et 350; | b) 147 et 490; | c) 308 et 364.

Exercice 34

Soit $n \in \mathbb{N}$, $a = n+3$ et $b = 2n+1$.

1. Montrez que si d divise a et b, alors d divise 5.

2. Quels sont les valeurs possibles du PGCD de a et b ?

3. Déterminez $a \wedge b$ selon les valeurs de n.

Exercice 35

Soient a et b des entiers naturels. On a $a = 630$, $a \wedge b = 105$ et $600 < b < 1\,100$. Trouvez b.
Même question avec 600, 12, 260 et 300 respectivement.

Exercice 36

Si on divise 2 897 et 3 505 par un même entier positif, on obtient respectivement 13 et 5 comme restes.
Quel est cet entier ?
Même question avec 4 294, 3 521, 10 et 11.

X - NOMBRES PREMIERS ENTRE EUX

a. Définition

Définition 4 Entiers premiers entre eux

Deux entiers a et b sont premiers entre eux si et seulement si

$$a \wedge b = 1$$

Par exemple, on vérifie à l'aide de la fonction gcd de XCAS (plus efficace que nos petits programmes) que 1234 et 258147 sont premiers entre eux

```
gcd(1234,258147)
```

b. Théorème de Bézout

D'après l'égalité de Bézout vue précédemment

Théorème 4 Théorème de Bézout
Les entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que $au+bv=1$

$$a\wedge b=1 \iff \text{il existe } (u,v)\in\mathbb{Z}^2 \text{ tel que } au+bv=1$$

On peut par exemple prouver ainsi que deux entiers consécutifs sont premiers entre eux car

$$n\times(-1)+(n+1)\times 1=1$$

c. Théorème de Gauss

Théorème 5 Théorème de Gauss
Si $a|bc$ et si $a\wedge b=1$ alors $a|c$

Il suffit d'utiliser le théorème de Bézout. je vous laisse le faire.
Par exemple 8 divise $3\times 16=48$ et 8 est premier avec 3 donc 8 divise 16 (on le savait !)
Mais 8 divise $6\times 4=24$ mais ne divise ni 6 ni 4.
Nous allons en donner un corrolaire souvent très utile

Corrolaire
Si un entier est divisibles par deux entiers a et b premiers entre eux, alors il est divisible par leur produit

Ainsi, pour prouver qu'un entier est divisible par 24, il suffit de prouver qu'il est divisible par 3 et 8 qui sont premiers entre eux.

d. Exercices

Exercice 37

Prouvez que $2n+1$ et $3n+2$ sont premiers entre eux.

Exercice 38

On suppose que a et b sont premiers entre eux. Prouvez que $a+b$ est premier avec a et b.

Exercice 39

On suppose que $a\wedge b=1$ et $a\wedge c=1$.

1. Montrez que $a\wedge bc=1$.

2. Montrez que $a^n\wedge b^p=1$ pour tous n et p dans $[\![1\,;+\infty[\![$.

Exercice 40

Trouvez a et b tels que $a+b=112$ et $a\wedge b=14$.

Exercice 41

On pose $a = 2n^3 + 5n^2 + 4n + 1$ et $b = 2n^2 + n$.

1. Prouvez que $2n+1$ divise a et b.

2. $2n+1$ est-il le PGCD de a et b ?

Exercice 42

Quatre entiers positifs a, b et c forment dans cet ordre une suite arithmétique dont la raison est un nombre entier premier avec a.
Trouvez ces nombres sachant que $10a^2 = d - b$.

Exercice 43

Prouvez que pour tout entier n, le nombre $A = n(5n^2+1)$ est divisible par 6.

XI - ÉQUATIONS DIOPHANTIENNES $ax + by = c$

Exercice 44 Exercice résolu

1. Nous voulons résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $1260x + 294y = 2814$
Aprés simplifications, nous obtenons l'équation équivalente

$$30x + 7y = 67 \quad (1)$$

Or $-3 \times 30 + 13 \times 7 = 1$, d'où $30 \times (-201) + 7 \times 871 = 67$ et donc

$$(1) \Longleftrightarrow 30(x+201) = 7(871 - y)$$

Mais 30 et 7 étant premiers entre eux, le théorème de Gauss nous permet d'affirmer que, si (x, y) est solution, alors 30 divise $871 - y$ et 7 divise $x + 201$. Les couples solutions sont donc de la forme $(-201 + 7k, 871 - 30k')$, $(k, k') \in \mathbb{Z}^2$. Remarquons ensuite que $k = k'$, puis que $871 = 29 \times 30 + 1$ et $-201 = -29 \times 7 + 2$, d'où

$$S = \left\{(-7p + 2, 30p + 1),\ p \in \mathbb{Z}\right\}$$

2. Si nous voulons faire la même chose avec l'équation $1260x + 294y = 3814$, nous remarquons qu'après division par 2, l'équation est équivalente à

$$(2 \times 3 \times 7) \times 45\, x + (2 \times 3 \times 7) \times 21\, y = 1907$$

Or 1907 n'est pas divisible par 2 donc $S = \emptyset$.

Exercice 45

Résolvez les équations suivantes dans $\mathbb{Z}^2$:

a) $41x-27y=1$
b) $5x-8y=2$
c) $-156x+276y=24$

XII - EXERCICES DIVERS

Exercice 46 Éléments inversibles de $\mathbb{Z}_n$

On note $\mathbb{Z}_n$ l'ensembles des classes modulo n. Par exemple, $\mathbb{Z}_3$ contient trois éléments : $\dot{0}$, $\dot{1}$ et $\dot{2}$.

1. a) À l'aide d'un tableur, dressez les tables de multiplication de $\mathbb{Z}_9$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{12}$ et $\mathbb{Z}_{13}$. Vous pourrez utiliser la fonction `MOD(nombre;divis` qui renvoie le reste de la division euclidienne de `nombre` par `diviseur`.

b) Vous avez par exemple obtenu $4\times 2\equiv 4\times 5[12]$. A-t-on pour autant $2\equiv 5[12]$?
Autre problème : on a $4\times 3\equiv 0[12]$, alors que ni 4 ni 3 n'est nul. On dit que 4 et 3 sont des diviseurs de zéro.
Observe-t-on les mêmes « anomalies » dans $\mathbb{Z}_9$? $\mathbb{Z}_{11}$? $\mathbb{Z}_{13}$?

c) Résolvez les équations $(E_1): 5x+7=0$, $(E_2): 6x-3=0$ et $(E_3): 3x+2=0$ dans $\mathbb{Z}_9$ puis dans $\mathbb{Z}_{13}$.

2. On recherche à présent les éléments inversibles de $\mathbb{Z}_n$.
0

Définition
On dit que $\dot{a}$ est inversible dans $\mathbb{Z}_n$ si et seulement s'il existe un élément $\dot{b}$ de $\mathbb{Z}_n$ tel que

$$\dot{a}\times\dot{b}=\dot{1}$$

a) Montrez que $\dot{a}$ est inversible dans $\mathbb{Z}_n$ si et seulement si a et n sont premiers entre eux.

Pensez au théorème de Bézout.

b) Commentez alors les résultats observés à la question 1).

c) On suppose à présent que $\dot{a}$ est inversible dans $\mathbb{Z}_n$. Déterminez son inverse dans $\mathbb{Z}_n$ en utilisant les résultats du a).

3. Première application : résolution d'équations.

a) Résolvez dans $\mathbb{Z}_{31}\times\mathbb{Z}_{31}$ le système $\begin{cases} 8x+7y &= 25\\ 13x+24y &= 17\end{cases}$

b) Résolvez dans $\mathbb{Z}_{4999}$ $2321x+1553=0$.

4. Deuxième application : chiffrement affine.

Voici notre premier contact avec la *cryptographie*, la science du secret. Elle occupe actuellement la pointe de la recherche, notamment en arithmétique car elle a des applications quotidiennes en perpétuelle évolution : internet, cartes à puce. Ce sont les militaires qui les premiers ont eu recours à l'arithmétique pour coder leurs messages. Les premières méthodes se contentaient de changer l'ordre des lettres. Par exemple, César numérotait les lettres de l'alphabet puis les décalait de trois rang : un a devenait un d, un r devenait un u, un z devenait un c. Nous allons étudier un système du même style.

On assimile les vingt-six lettres de l'alphabet auxquelles on ajoute l'espace aux nombres 0, 1,...,26. On code ces nombres à l'aide d'une fonction f du type :

$$f\ :\ x\mapsto ax+b[27]$$

où a et b sont des entiers.

a) Étude d'un cas particulier : $f(x)=17x+22[27]$.

a) Proposez une table de chiffrage à l'aide d'un tableur.

a) Chiffrez « LA MAITRESSE EN MAILLOT DE BAIN ».

a) Déterminez, s'il existe, l'inverse u de 17 dans $\mathbb{Z}_{27}$.

a) On veut trouver une fonction de déchiffrage g qui vérifierait

$$y \equiv f(x)[27] \Longleftrightarrow g(y) \equiv x[27]$$

En quoi le résultat précédent peut vous aider à déterminer g ?

b) Reprenez les questions précédentes avec $f\ :\ x \mapsto 9x+22[27]$

c) Montrez que, pour pouvoir déterminer une fonction de déchiffrage, il faut et il suffit que a soit premier avec 27.

Exercice 47 Le chiffrement de Lester Hill

Dans les années 20, le bon Lester essaya de mettre un peu de piquant dans le chiffrement de César. On commence par supprimer espaces et ponctuations et on associe comme d'habitude chaque lettre à un nombre de $[\![0\,,25]\!]$. L'innovation de Lester est de ne pas chercher à coder le message lettre par lettre, mais groupe de lettre par groupe de lettre. Nous allons étudier le cas particulier des blocs de deux lettres qu'on appellera *bigrammes*.
La clé secrète du cryptosystème est cette fois-ci constitué de quatre entiers a, a', b et b' tels que le système

$$\left\{\begin{array}{rcl} ax+by & \equiv & c[26] \\ a'x+b'y & \equiv & c'[26] \end{array}\right.$$

admette toujours une solution unique dans $[\![0\,,25]\!] \times [\![0\,,25]\!]$, quels que soient c et c'.
Pour un bigramme, on remplace x et y par les deux nombres correspondant aux lettres du bigramme. On en déduit les deux nombres c et c' que l'on remplace ensuite par les deux lettres correspondantes.
Si le nombre de lettres du message est impair, on convient de remplacer la dernière par X.

1. Exemple : avec la clé $a=8$, $b=3$, $a'=5$, $b'=2$, codez « TURLUTUTU ».

2. Démontrez que le système correspondant à la clé précédente admet toujours des solutions, quels que soient c et c'.

3. Décodage : débrouillez-vous pour donner les formules qui permettent de décoder (nous avons déjà résolu ce genre de problème dans l'exercice 20).

4. Cas général : démontrez que le système admet toujours des solutions si $ab'-a'b$ et 26 sont premiers entre eux.

Exercice 48 Le problème du ministre syldave.

En vue d'intégrer la Confédération Internationale de la Consommation, le ministre syldave des finances engage un conseiller étranger qui lui propose, par mesure d'économie, de ne frapper que des pièces de 4999 Spchprzts et de 3771 Spchprzts. Un dialogue s'engage :
- Mais, mon cher Joe Max Bill Pol, comment pourrai-je acheter mon pichet de bière Zmtschgr à un Spchprzts ?
- No problem Otto : il souffit que le gawçon vous wende la money.
- Soit, mais sera-ce possible pour n'importe quelle somme ?
- Absolutely dear.

Expliquez !

Exercice 49 Le problème de l'astronome syldave.

Otto Blortsch, le célèbre astronome syldave, a observé au jour J_0 la comète Arzchtrpm (qu'on notera A), qui, comme chacun sait, apparaît périodiquement tous les 105 jours. Six jours plus tard, il observe la comète Brtdszztch (qu'on notera B) qui, bien sûr, a une période d'apparition de 81 jours. Otto voudrait déterminer J_1, le jour de la prochaine apparition *simultanée* des deux comètes à ses yeux ébaubis.

1. Soient u et v (tiens tiens...) le nombre de périodes effectuées respectivement par A et B entre J_0 et J_1. Montrez que le couple (u,v) est solution de l'équation

$$(E)\ :\ 35x-27y=2$$

.

2. Déterminez UNE solution particulière de (E), puis TOUTES les solutions.
3. Déterminez LA solution correspondant à J_1.
4. Le jours J_0 était le dimanche 7 décembre 2003. Quelle fut (ou sera) la date exacte de J_1 ?
5. Ce jour-là, Otto avait une gastro et a raté l'événement : combien de jours devra-t-il attendre jusqu'à la prochaine conjonction des deux astres ?

Exercice 50 Le problème des pirates syldaves.

15 pirates syldaves se partagent un butin constitué de pièces d'or. Mais une fois le partage (équitable) effectué, il reste 3 pièces. Que va-t-on en faire ? La discussion s'anime. Bilan : 8 morts. Les survivants recommencent le partage, et il reste cette fois-ci 2 pièces ! Nouvelle bagarre à l'issue de laquelle il ne reste que 4 pirates. Heureusement, ils peuvent cette fois-ci se partager les pièces sans qu'il n'en reste aucune. Sachant que 32 Zmtschgr (bière syldave) coûtent une pièce d'or, combien (au minimum) de Zmtschgr pourra boire chaque survivant ?

Exercice 51 Numéro I.S.B.N.

L'*International Standard Book Number* est un numéro qui sert à identifier un livre. Ce numéro est un « mot » de longueur 10 constitué avec les chiffres $0, 1, \cdots, 9$ et la lettre X (qui représente le nombre 10). La lettre X ne sera utilisée, si nécessaire, que pour la clé qui est le dernier caractère.

Exemples : 2 84180 013 X, ou 0 12 163251 2.

Le premier chiffre représente le pays, ensuite un bloc de chiffres est attribué à un éditeur, puis un autre bloc est le numéro donné par l'éditeur au livre. Le dernier caractère est la clé, calculée de telle sorte que si $a_1 a_2 \cdots a_{10}$ désigne un numéro I.S.B.N., l'entier $\sum_{i=1}^{10} i\,a_{11-i}$ soit divisible par 11.

1. Montrer que les neuf premiers chiffres d'un numéro I.S.B.N. étant donnés, il y a une seule manière de déterminer la clé.
2. On suppose que lors de la saisie d'un numéro I.S.B.N., on effectue un erreur sur un (et un seul) des 10 caractères. Montrer que l'on peut détecter l'erreur mais pas la corriger.
3. On suppose que lors de la saisie d'un numéro I.S.B.N., on permute deux des caractères sans modifier les autres. Montrer que l'on peut détecter l'erreur mais pas la corriger.
4. Pourquoi prendre $\sum_{i=1}^{10} i\,a_{11-i}$ plutôt que $\sum_{i=1}^{10} a_i$?

Exercice 52 Arithmétique...complexe.

Soit a un nombre complexe. On note $\mathbb{Z}[a]$ l'ensemble des complexes z qui s'écrivent sous la forme $z = x + ay$ avec x et y des entiers. Plus sommairement on écrit

$$\mathbb{Z}[a] = \{z = x + ay \,|\, x, y \in \mathbb{Z}\}$$

A - Structure d'anneau - Éléments inversibles

1. Vérifiez que $\mathbb{Z}[a]$ contient 0, que si z et z' appartiennent à $\mathbb{Z}[a]$, il en est de même pour $z - z'$. On dit alors que $\mathbb{Z}[a]$ muni de l'addition a une structure de *groupe*.
2. Vérifiez que $\mathbb{Z}[a]$ contient 1 et que si z et z' appartiennent à $\mathbb{Z}[a]$, il en est de même pour leur produit zz'. Sachant que la multiplication des complexes est distributive sur l'addition, on dit alors que $\mathbb{Z}[a]$ muni de l'addition et de la multiplication a une structure *d'anneau*.
3. Petit rappel : on dit que z est inversible dans A si et seulement s'il existe un élément z' de A tel que $zz' = 1$.
a) Trouvez par exemple les éléments inversibles de $\mathbb{Z}[0]$[n].
b) Quels sont les éléments inversibles de $\mathbb{Z}[i]$[o] ?

[n] Au fait, comment écrit-on plus simplement $\mathbb{Z}[0]$?
[o] Utilisez les modules

B - Division euclidienne dans $\mathbb{Z}[i]$

On va s'intéresser à l'existence d'une division euclidienne dans l'anneau $\mathbb{Z}[i]$, c'est à dire l'existence, pour tout couple (z,w) d'éléments de $\mathbb{Z}[i]$ avec $w \neq 0$, d'un couple (q,r) d'éléments de $\mathbb{Z}[i]$ tel que

$$z = wq + r \quad \text{avec} \quad |r| < |w|$$

1. On considère le plan complexe muni d'un repère orthonormé $\left(O; \vec{u}, \vec{v}\right)$. Comment décririez-vous les images des éléments de $\mathbb{Z}[i]$?

2. On appelle f le complexe égal à z/w. Est-ce que f appartient forcément à $\mathbb{Z}[i]$?

3. On note $f = x + iy$ avec x et y des réels et F son image dans le plan complexe. Soit Q l'image de q dans le plan complexe. Traduisez graphiquement la division euclidienne de z par w.

4. Comment caractérisez par une inégalité l'entier a « le plus proche » de x ?

5. Soit b l'entier le plus proche de y. Notons q le complexe $a + ib$. Montrez que $|f - q| < 1$ et concluez notre petite étude.

C- Le théorème de Bézout mis en défaut dans $\mathbb{Z}[i\sqrt{5}]$?

Nous aurons besoin de deux définitions pour travailler

Définition 1

Deux éléments d'un anneau A sont dits premiers entre eux s'ils n'ont pas de diviseur commun non inversible (i.e. si tous leurs diviseurs communs sont inversibles).

Définition 2

On dit que deux éléments a et b d'un anneau A sont étrangers s'ils vérifient

$$\lambda a + \mu b = 1 \quad \text{avec} \quad \lambda, \mu \in A$$

Dans la suite de l'exercice, on travaillera dans $\mathbb{Z}[i\sqrt{5}]$ qu'on notera A.

1. Montrez que la définition 1 est compatible avec la définition donnée dans le cours pour $\mathbb{Z}$.

2. Quels sont les éléments inversibles de A ?

3. Montrez que $4 + i\sqrt{5}$ et $4 - i\sqrt{5}$ sont étrangers dans A.

4. Quels sont les diviseurs de 3 dans A ?

5. Montrez alors que $4 + i\sqrt{5}$ et 3 sont premiers entre eux ?

6. Montrez qu'ils ne sont pas étrangers.

7. Commentez ce dernier résultat.

Exercice 53 Utilisation de la base 2 pour accélérer le calcul de x^n

Pour calculer x^{15}, on fait 14 multiplications : $x \times x \times \cdots \times x$. Si on décompose 15 en base 2, on peut économiser des calculs

$$15 = 2^3 + 2^2 + 2^1 + 2^0$$

donc

$$x^{15} = \left((x^2)^2\right)^2 \times (x^2)^2 \times x^2 \times x$$

On calcule x^2 puis $x^4 = (x^2)^2$ puis $x^8 = (x^4)^2$ et enfin

$$x^{15} = x \times x^2 \times x^4 \times x^8$$

soit 6 multiplications au lieu de 14.
Nous verrons bientôt que l'arithmétique est intimement liée à l'algorithmique : plus on économisera notre ordinateur, plus il aura de « place » pour résoudre notre problème.
Malgré tout, le calcul de x^k en lui-même n'a que peu d'intérêt. Ce qui nous sera plus utile, c'est de trouver un algorithme calculant $rapidement\ x^k$ modulo n. Il faut évidemment éviter de calculer d'abord x^k puis de regarder sa classe modulo n. Il vaut mieux travailler à chaque étape modulo n pour ne pas introduire des nombres gigantesques.
Voici un petit programme calculant x^k modulo n en s'inspirant de la méthode vue plus haut.

X $\leftarrow x$
K $\leftarrow k$
N $\leftarrow n$
A $\leftarrow 1$
while K>0 **do**

  if K est pair **then**
    X $\leftarrow$ X $*$ X mod N
    K $\leftarrow$ K/2
  else
    A $\leftarrow$ A $*$ X mod N
    K $\leftarrow$ K $-$ 1
  end if
end while
return A

1. Expliquez le fonctionnement de cet algorithme.
2. Faîtes pas à pas le calcul de x^{15} tel que le ferait un ordinateur obéissant à ce programme.
3. Proposer un programme s'adaptant à votre calculatrice ou à Mupad.
4. Voici ce que ça donne sur XCAS.

```
Puissance(x,k,n):={
local X,K,A;
X:=x; K:=k; A:=1;
while(K>0){
if (irem(K,2)=0) {X:=X*X;K:=K/2;}
 else {A:=irem(A*X,n); K:=K-1;}
}
return(A);
}
```

On appelle

```
Puissance(2412,1137,57)
```

et on obtient 18.

Remarque 0.2 : *Bien sûr, XCAS fait ça tout seul grâce à* **powmod**(a,n,p)...

Exercice 54 Algorithme des différences

1. Soit a et b deux entiers naturels non nuls. Montrez que $a \wedge b = b \wedge (a-b)$
2. Utilisez cette remarque pour déterminer un algorithme calculant le PGCD de deux entiers naturels non nuls[p]. Testez-le sur votre machine ou XCAS.

Exercice 55 Algorithme d'Euclide

Je vous rappelle que $a \wedge b$ est le dernier reste non nul obtenu par l'algorithme d'Euclide. Déterminez un algorithme donnant

[p] $a_0 = max(a,b)$, $b_0 = min(a,b)$ et $b_{n+1} = min(a_n, b_n)$, $a_{n+1} = |a_n - b_n|$. Montrez que (b_n) est nulle à partir d'un certain rang

$a \wedge b$ à partir de l'algorithme d'Euclide. Vous n'utiliserez que les opérations usuelles et la fonction « partie entière » de votre calculatrice
Cet algorithme est-il plus efficace que celui de l'exrcice précédent ?

Exercice 56 Calcul des coefficients de Bézout par la méthode de Borel

On suppose que a et b sont premiers entre eux et on cherche deux entiers u et v vérifiant $au+bv=1$.
On s'amuse à calculer les multiples successifs de a et leur reste dans la division euclidienne par b.
En quoi ce petit jeu peut nous permettre d'obtenir u et v ? Peut-il y avoir problème ?
Déterminez un algorithme permettant de calculer u et v.

Exercice 57 Algorithme d'Euclide étendu avec un tableur

Comme nous l'avons vu en cours, à chaque étape de l'algorithme d'Euclide, nous pouvons exprimer le reste r_n en fonction de a et b

$$r_n = u_n a + v_n b$$

1. On part de $a = bq_1 + r_2$, $r_0 = a$, $r_1 = b$. Sachant qu'à la p-ième division on a

$$r_{p-1} = r_p q_p + r_{p+1}$$

montrez que

$$\begin{cases} u_{p+1} &= u_{p-1} - q_p u_p \\ v_{p+1} &= v_{p-1} - q_p v_p \end{cases}$$

2. Déduisez-en un « programme » permettant de déterminer deux entiers u et v tels que

$$ua + vb = 1$$

à l'aide d'un tableur.

Exercice 58 Le tableur décode complètement

Nous allons résoudre l'exercice XXI à l'aide du tableur XCAS et de deux de ses fonctions :

- `asc(A1)` qui renvoie le code ASCII du premier caractère écrit dans la cellule A1. Le code de A est 65, celui de B est 66, ... , celui de Z est 90. Par commodité, nous remplacerons l'espace par @ qui a pour code 64;
- `char(A1)` qui renvoie le caractère associé au code ASCII rentré en A1.

Mettez au point un codeur où vous afficherez le message à coder sur la première ligne, le message « chiffré » où vous aurez remplacé chaque lettre par son code sur la deuxième ligne, appliquez f sur la troisième ligne en utilisant la fonction `irem`, puis le message codé sur la quatrième ligne.

De la même manière, mettez au point un décodeur et vérifiez les résultats trouvés à l'exercice XXI.

XIII - PPCM

Théorème 6

L'ensemble des multiples strictement positifs communs à a et b admet un plus petit élément qu'on appelle **plus petit multiple commun** de a et b. On le note PPCM(a,b) ou $a \vee b$

Pour la preuve, on utilise la propriété des parties de $\mathbb{N}$ non vides et minorées.

Propriété14

Soient a et b deux entiers positifs, d leur pgcd. Il existe deux entiers a' et b' tels que $a = da'$ et $b = db'$. De plus a' et b' sont premiers entre eux.

En reprenant les divisions de l'algorithme d'Euclide, on prouve que

$$ka \wedge kb = k(a \wedge b)$$

donc $a' \wedge b' = \dfrac{a}{d} \wedge \dfrac{b}{d} = \dfrac{1}{d}d = 1$

Théorème 7

$(a \wedge b)(a \vee b) = ab$

On note $m = a \vee b$ et $d = a \wedge b$. Alors il existe deux entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$. Soit M un multiple commun de a et b, alors il existe deux entiers u et v tels que M $= au = bv = da'u = db'v$. Or d est non nul, donc

$$a'u = b'v$$

L'intérêt réside dans le fait que a' et b' sont premiers entre eux (c'est pourquoi cette méthode est souvent utilisée en exercice). On peut donc utiliser le magique théorème de Gauss a' divisant $b'v$, a' divise v, donc il existe un entier k tel que $v = a'k$.
Tout ceci pour dire que tout multiple commun M de a et b s'écrit *nécessairement* sous la forme M $= db'a'k$.

Réciproquement, tout nombre s'écrivant sous la forme $db'a'k$ avec k un naturel quelconque est un multiple commun de a et de b car

$$db'a'k = b(a'k) = a(b'k)$$

Donc les multiples communs de a et de b SONT les multiples de $da'b'$. Le plus petit multiple de $da'b'$ étant $da'b'$ lui-même, on en déduit finalement que

$$a \vee b = da'b'$$

Ainsi $(a \wedge b)(a \vee b) = d \cdot da'b' = da' \cdot db' = ab$

Propriété15

Si k est un entier naturel, alors $ka \vee kb = k(a \vee b)$

La démonstration utilise le théorème précédent et la propriété : $ka \wedge kb = k(a \wedge b)$.

Un exemple corrigé

On cherche les entiers naturels non nuls a et b vérifiant $\begin{cases} a^2 - b^2 = 405 \\ 3(a \vee b) = ab \end{cases}$

Il est assez naturel d'utiliser le théorème précédent : $(a \wedge b)(a \vee b) = ab$. Les entiers a et b étant non nuls, il en est de même de leur ppcm, donc $a \wedge b = 3$, ce qui nous permet d'introduire les entiers a' et b' vérifiant $a = 3a'$ et $b = 3b'$: ils ont en effet l'énorme avantage d'être premiers entre eux.
La première équation devient donc après simplification $a'^2 - b'^2 = 45$, c'est à dire

$$(a' - b')(a' + b') = 45$$

En effet, les carrés nous ennuient, mais on peut discuter sur le produit de deux entiers en parlant diviseur. Il existe en effet peu de diviseurs de 45 : 1, 3, 5, 9, 15 et 45 lui-même. De plus, a' et b' étant positifs, $a' - b'$ l'est aussi et $a' - b' \leqslant a' + b'$. Envisageons donc les différents cas

- $a' - b' = 1$ et $a' + b' = 45$, alors $a' = 23$ et $b' = 22$ conviennent.
- $a' - b' = 3$ et $a' + b' = 15$, alors $a' = 9$ et $b' = 6$ mais ils ne sont pas premiers entre eux.
- $a' - b' = 5$ et $a' + b' = 9$, alors $a' = 7$ et $b' = 2$ conviennent.

Il ne peut y avoir d'autres solutions et celles-ci conviennent, donc les couples solution sont (21,6) et (69,66).

Exercice 59

trouvez tous les entiers a et b tels que la différence entre leur PPCM et leur PGCD est égal à 187.

Exercice 60

On cherche les entiers naturels non nuls a et b vérifiant $\begin{cases} a \wedge b = 18 \\ a \vee b = 108 \end{cases}$

XIV - Exercices de Bac

Exercice 61

Pour coder un message, on procède de la manière suivante : à chacune des 26 lettres de l'alphabet, on commence par associer un entier n de l'ensemble
$\Omega = \{0\ ;\ 1\ ;\ 2\ ;\ \ldots\ ;\ 24\ ;\ 25\}$ selon le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

a et b étant deux entiers naturels donnés, on associe à tout entier n de Ω le reste de la division euclidienne de $(an+b)$ par 26 ; ce reste est alors associé à la lettre correspondante.
Exemple : pour coder la lettre P avec $a=2$ et $b=3$, on procède de la manière suivante :
étape 1 : on lui associe l'entier $n=15$.
étape 2 : le reste de la division de $2\times 15+3=33$ par 26 est 7.
étape 3 : on associe 7 à H. Donc P est codé par la lettre H.

1. Que dire alors du codage obtenu lorsque l'on prend $a=0$?

2. Montrer que les lettres A et C sont codées par la même lettre lorsque l'on choisit $a=13$.

3. *Dans toute la suite de l'exercice*, on prend $a=5$ et $b=2$.

a) On considère deux lettres de l'alphabet associées respectivement aux entiers n et p. Montrer, que si $5n+2$ et $5p+2$ ont le même reste dans la division par 26 alors $n-p$ est un multiple de 26. En déduire que $n=p$.

b) Coder le mot AMI.

4. On se propose de décoder l a lettre E.

a) Montrer que décoder la lettre E revient à déterminer l'élément n de Ω tel que $5n-26y=2$, où y est un entier.

b) On considère l'équation $5x-26y=2$, avec x et y entiers relatifs.

b) Donner une solution particulière de l'équation $5x-26y=2$.

b) Résoudre alors l'équation $5x-26y=2$.

b) En déduire qu'il existe un unique couple $(x\ ;\ y)$ solution de l'équation précédente, avec $0\leqslant x\leqslant 25$.

c) Décoder alors la lettre E.

Exercice 62

1. a) Déterminer suivant les valeurs de l'entier naturel non nul n le reste dans la division euclidienne par 9 de 7^n.

b) Démontrer alors que $(2005)^{2005} \equiv 7\ (9)$.

2. a) Démontrer que pour tout entier naturel non nul n : $(10)^n \equiv 1\ (9)$.

b) On désigne par N un entier naturel écrit en base dix, on appelle S la somme de ses chiffres.
Démontrer la relation suivante : $N \equiv S\ (9)$.

c) En déduire que N est divisible par 9 si et seulement si S est divisible par 9.

3. On suppose que $A = (2005)^{2005}$; on désigne par :
- B la somme des chiffres de A ;
- C la somme des chiffres de B ;
- D la somme des chiffres de C.

a) Démontrer la relation suivante : $A \equiv D\ (9)$.

b) Sachant que $2005 < 10000$, démontrer que A s'écrit en numération décimale avec au plus 8020 chiffres. En déduire que $B \leqslant 72180$.

c) Démontrer que $C \leqslant 45$.

d) En étudiant la liste des entiers inférieurs à 45, déterminer un majorant de D plus petit que 15.

e) Démontrer que $D = 7$.

Exercice 63

Partie A

Soit N un entier naturel, impair non premier.
On suppose que $N = a^2 - b^2$ où a et b sont deux entiers naturels.

1. Montrer que a et b n'ont pas la même parité.

2. Montrer que N peut s'écrire comme produit de deux entiers naturels p et q.

3. Quelle est la parité de p et de q ?

Partie B

On admet que 250 507 n'est pas premier.
On se propose de chercher des couples d'entiers naturels $(a\,;\,b)$ vérifiant la relation

$$\text{(E)} : \quad a^2 - 250507 = b^2.$$

1. Soit X un entier naturel.

a) Donner dans un tableau, les restes possibles de X modulo 9 ; puis ceux de X^2 modulo 9.

b) Sachant que $a^2 - 250507 = b^2$, déterminer les restes possibles modulo 9 de $a^2 - 250507$; en déduire les restes possibles module 9 de a^2.

c) Montrer que les restes possibles modulo 9 de a sont 1 et 8.

2. Justifier que si le couple $(a\,;\,b)$ vérifie la relation (E), alors $a \geqslant 501$. Montrer qu'il n'existe pas de solution du type $(501\,;\,b)$.

3. On suppose que le couple $(a\,;\,b)$ vérifie la relation (E).

a) Démontrer que a est congru à 503 ou à 505 modulo 9.

b) Déterminer le plus petit entier naturel k tel que le couple $(505+9k\,;\,b)$ soit solution de (E), puis donner le couple solution correspondant.

Partie C

1. Déduire des parties précédentes une écriture de 250 507 en un produit deux facteurs.

2. Les deux facteurs sont-ils premiers entre eux ?

3. Cette écriture est-elle unique ?

Exercice 64

Dans cet exercice, on pourra utiliser le résultat suivant :
« Étant donnés deux entiers naturels a et b non nuls, si PGCD$(a\,;\,b)=1$ alors PGCD$(a^2\,;\,b^2)=1$ ».
Une suite (S_n) est définie pour $n>0$ par $S_n=\sum_{p=1}^{n} p^3$. On se propose de calculer, pour tout entier naturel non nul n, le plus grand commun diviseur de S_n et S_{n+1}.

1. Démontrer que, pour tout $n>0$, on a : $S_n=\left(\dfrac{n(n+1)}{2}\right)^2$.

2. Étude du cas où n est pair. Soit k l'entier naturel non nul tel que $n=2k$.

a) Démontrer que PGCD$(S_{2k}\,;S_{2k+1})=(2k+1)^2$PGCD$\left(k^2\,;\,(k+1)^2\right)$.

b) Calculer PGCD $(k\,;\,k+1)$.

c) Calculer PGCD$(S_{2k}\,;S_{2k+1})$.

3. Étude du cas où n est impair. Soit k l'entier naturel non nul tel que $n=2k+1$.

a) Démontrer que les entiers $2k+1$ et $2k+3$ sont premiers entre eux.

b) Calculer PGCD$(S_{2k+1}\,;S_{2k+2})$.

4. Déduire des questions précédentes qu'il existe une unique valeur de n, que l'on déterminera, pour laquelle S_n et S_{n+1} sont premiers entre eux.

Exercice 65

On considère la suite (u_n) d'entiers naturels définie par

$$\begin{cases} u_0 &= 14 \\ u_{n+1} &= 5u_n-6 \text{ pour tout entier naturel } n \end{cases}$$

1. Calculer u_1, u_2, u_3 et u_4.
Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n ?

2. Montrer que, pour tout entier naturel n, $u_{n+2}\equiv u_n \pmod 4$.
En déduire que pour tout entier naturel k, $u_{2k}\equiv 2 \pmod 4$ et
$u_{2k+1}\equiv 0 \pmod 4$.

a) Montrer par récurrence que, pour tout entier naturel n,
$2u_n=5^{n+2}+3$.

b) En déduire que, pour tout entier naturel n, $2u_n\equiv 28 \pmod{100}$.

3. Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n.

4. Montrer que le PGCD de deux termes consécutifs de la suite (u_n) est constant. Préciser sa valeur.

Exercice 66

On appelle (E) l'ensemble des entiers naturels qui peuvent s'écrire sous la forme $9+a^2$ où a est un entier naturel non nul ; par exemple $10=9+1^2$; $13=9+2^2$ etc.
On se propose dans cet exercice d'étudier l'existence d'éléments de (E) qui sont des puissances de 2, 3 ou 5.

1. Étude de l'équation d'inconnue a : $a^2+9=2^n$ où $a\in\mathbb{N}$, $n\in\mathbb{N}$, $n\geqslant 4$.

a) Montrer que si a existe, a est impair.

b) En raisonnant modulo 4, montrer que l'équation proposée n'a pas de solution.

2. Étude de l'équation d'inconnue a : $a^2+9=3^n$ où $a\in\mathbb{N}$, $n\in\mathbb{N}$, $n\geqslant 3$.

a) Montrer que si $n\geqslant 3$, 3^n est congru à 1 ou à 3 modulo 4.

b) Montrer que si a existe, il est pair et en déduire que nécessairement n est pair.

c) On pose $n=2p$ où p est un entier naturel, $p\geqslant 2$. Déduire d'une factorisation de 3^n-a^2, que l'équation proposée n'a pas de solution.

3. Étude de l'équation d'inconnue a : $a^2+9=5^n$ où $a\in\mathbb{N}$, $n\in\mathbb{N}$, $n\geqslant 2$.

a) En raisonnant modulo 3, montrer que l'équation n'a pas de solution si n est impair.

b) On pose $n=2p$, en s'inspirant de **2. c.** démontrer qu'il existe un unique entier naturel a tel que a^2+9 soit une puissance entière de 5.

Exercice 67

Les suites d'entiers naturels (x_n) et (y_n) sont définies sur $\mathbb{N}$ par :

$$x_0=3 \quad \text{et} \quad x_{n+1}=2x_n-1$$
$$y_0=1 \quad \text{et} \quad y_{n+1}=2y_n+3.$$

1. Démontrer par recurrence que pour tout entier naturel n, $x_n=2^{n+1}+1$.

2. a) Calculer le pgcd de x_8 et x_9, puis celui de x_{2002} et x_{2003}. Que peut-on en déduire pour x_8 et x_9 d'une part, pour x_{2002} et x_{2003} d'autre part ?

b) x_n et x_{n+1} sont-ils premiers entre eux pour tout entier naturel n ?

3. a) Démontrer que pour tout entier naturel n, $2x_n-y_n=5$.

b) Exprimer y_n en fonction de n.

c) En utilisant les congruences modulo 5, étudier suivant les valeurs de l'entier naturel p le reste de la division euclidienne de 2^p par 5.

d) On note d_n le pgcd de x_n et y_n pour tout entier naturel n.
Démontrer que l'on a $d_n=1$ ou $d_n=5$; en déduire l'ensemble des entiers naturels n tels que x_n et y_n soient premiers entre eux.

Exercice 68

On considère deux entiers naturels, non nuls, x et y premiers entre eux.
On pose S $=x+y$ et P $=xy$.

1. a) Démontrer que x et S sont premiers entre eux, de même que y et S.

b) En déduire que S $=x+y$ et P $=xy$ sont premiers entre eux.

c) Démontrer que les nombres S et P sont de parités différentes (l'un pair, l'autre impair).

2. Déterminer les diviseurs positifs de 84 et les ranger par ordre croissant.

3. Trouver les nombres premiers entre eux x et y tels que : SP $=84$.

4. Déterminer les deux entiers naturels a et b vérifiant les conditions suivantes :

$$\begin{cases} a+b &= 84 \\ ab &= d^3 \end{cases} \quad \text{avec } d=\text{pgcd}(a;b)$$

(On pourra poser $a=dx$ et $b=dy$ avec x et y premiers entre eux)

Exercice 69

1. On considère l'équation (1) d'inconnue $(n,\ m)$ élément de $\mathbb{Z}^2$:

$$11n - 24m = 1.$$

a) Justifier, à l'aide de l'énoncé d'un théorème, que cette équation admet au moins une solution.

b) En utilisant l'algorithme d'Euclide, déterminer une solution particulière de l'équation (1).

c) Déterminer l'ensemble des solutions de l'équation (1).

2. recherche du P.G.C.D. de $10^{11}-1$ et $10^{24}-1$.

a) Justifier que 9 divise $10^{11}-1$ et $10^{24}-1$.

b) $(n,\ m)$ désignant un couple quelconque d'entiers naturels solutions de (1), montrer que l'on peut écrire

$$\left(10^{11n}-1\right) - 10\left(10^{24m}-1\right) = 9.$$

c) Montrer que $10^{11}-1$ divise $10^{11n}-1$.
(on rappelle l'égalité $a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} + \cdots + a^0\right)$, valable pour tout entier naturel n non nul).
Déduire de la question précédente l'existence de deux entiers N et M tels que :

$$\left(10^{11}-1\right)\mathrm{N} - \left(10^{24}-1\right)\mathrm{M} = 9.$$

d) Montrer que tout diviseur commun à $10^{24}-1$ et $10^{11}-1$ divise 9.

e) Déduire des questions précédentes le P.G.C.D. de $10^{24}-1$ et $10^{11}-1$.

Exercice 70

Pour tout entier naturel n supérieur ou égal à 5, on considère les nombres

$$a = n^3 - n^2 - 12n \qquad \text{et} \qquad b = 2n^2 - 7n - 4.$$

1. Montrer, après factorisation, que a et b sont des entiers naturels divisibles par $n-4$.

2. On pose $\alpha = 2n+1$ et $\beta = n+3$. On note d le PGCD de α et β.

a) Établir une relation entre α et β indépendante de n.

b) Démontrer que d est un diviseur de 5.

c) Démontrer que les nombres α et β sont multiples de 5 si et seulement si $n-2$ est multiple de 5.

3. Montrer que $2n+1$ et n sont premiers entre eux.

4. a) Déterminer, suivant les valeurs de n et en fonction de n, le PGCD de a et b.

b) Vérifier les résultats obtenus dans les cas particuliers $n = 11$ et $n = 12$.

Exercice 71

1. On cherche deux entiers relatifs x et y solutions de l'équation (1) $ax+by = 60$ (a et b entiers naturels donnés tels que $ab \neq 0$).
On notera d le plus grand commun diviseur de a et b.

a) On suppose que l'équation (1) a au moins une solution $(x_0\ ;\ y_0)$. Montrer que d divise 60.

b) On suppose que d divise 60. Prouver qu'il existe alors au moins une solution $(x_0\ ;\ y_0)$ à l'équation (1).

2. On considère l'équation : (2) $\quad 24x+36y=60.$ (x et y entiers relatifs).

a) Donner le PGCD de 24 et 36 en justifiant brièvement. Simplifier l'équation (2).

b) Trouver une solution évidente pour l'équation (2) et résoudre cette équation. On appellera S l'ensemble des couples $(x\,;\,y)$ solutions.

c) Énumérer tous les couples $(x\,;\,y)$ solutions de (2) et tels que :

$$-10 \leqslant x \leqslant 10.$$

Donner parmi eux, ceux pour lesquels x et y sont multiples de 5.

d) Dans le plan rapporté à un repère orthonormal (unité graphique : 1 cm), représenter l'ensemble E des points M de coordonnées $(x\,;\,y)$ telles que :

$$\begin{cases} x &= 1+3t \\ y &= 1-2t \end{cases} \quad t \in \mathbb{R}.$$

e) Montrer que les points ayant pour coordonnées les solutions $(x;y)$ de l'équation (2) appartiennent à E.
Comment peut-on caractériser S ?

Exercice 72

Dans tout l'exercice, n désigne un entier naturel non nul.

1. a) Pour $1 \leqslant n \leqslant 6$, calculer les restes de la division euclidienne de $3n$ par 7.

b) Démontrer que, pour tout n, $3^{n+6}-3^n$ est divisible par 7.
En déduire que 3^n et 3^{n+6} ont le même reste dans la division par 7.

c) À l'aide des résultats précédents, calculer le reste de la division euclidienne de $3^{1\,000}$ par 7.

d) De manière générale, comment peut-on calculer le reste de la division euclidienne de 3^n par 7, pour n quelconque ?

e) En déduire que, pour tout entier naturel $n, 3^n$ est premier avec 7.

2. Soit $\mathrm{U}_n = 3+3^2+\cdots+3^{n-1} = \sum_{i=0}^{i=n-1} 3^i$, où n est un entier naturel supérieur ou égal à 2.

a) Montrer que si U^n est divisible par 7, alors 3^n-1 est divisible par 7.

b) Réciproquement, montrer que si 3^n-1 est divisible par 7, alors U_n est divisible par 7.
En déduire les valeurs de n telles que U_n soit divisible par 7.

Exercice 73

On considère l'équation

$$(1) \quad : \quad 20b-9c=2.$$

où les inconnues b et c appartiennent à l'ensemble $\mathbb{Z}$ des nombres entiers relatifs.

1. a) Montrer que si le couple $(b_0\,;\,c_0$ d'entiers relatifs est une solution de l'équation (1), alors c_0 est un multiple de 2.

b) On désigne par d le p.g.c.d. de $|b_0|$ et $|c_0|$. Quelles sont les valeurs possibles de d ?

2. Déterminer une solution particulière de l'équation (1), puis déterminer l'ensemble des solutions de cette équation.

3. Déterminer l'ensemble des solutions $(b\,;\,c)$ de (1) telles que p.g.c.d.$(b\,;\,c) = 2$.

4. Soit r un nombre entier naturel supérieur ou égal à 2. Le nombre entier naturel P, déterminé par

$$\mathrm{P} = \alpha_n r^n + \alpha_{n-1} r^{n-1} + \ldots + \alpha_1 r + \alpha_0$$

, où α_n, α_{n-1}, ...,α_1, α_0 sont des nombres entiers naturels vérifiant $0 < \alpha_n < r$, $0 \leqslant \alpha_{n-1} < r$,..., $0 \leqslant$, $\alpha_0 < r$ est noté $\overline{\alpha_n\alpha_{n-1}\ldots\alpha_1\alpha_0}^{(r)}$; cette écriture est dite « écriture de P en base r ». Soit P un nombre entier naturel s'écrivant $\overline{ca5}^{(6)}$ et $\overline{bbaa}^{(4)}$ (en base six et en base quatre respectivement).
Montrer que $a+5$ est un multiple de 4 et en déduire les valeurs de a, puis de b et de c.
Donner l'écriture de P dans le système décimal.

Exercice 74

1. On considère l'équation (E) : $8x+5y=1$, où $(x\,;\,y)$ est un couple de nombres entiers relatifs.

a) Donner une solution particulière de l'équation (E).

b) Résoudre l'équation (E).

2. Soit N un nombre naturel tel qu'il existe un couple $(a\,;\,b)$ de nombres entiers vérifiant : $\begin{cases} \mathrm{N} = 8a+1 \\ \mathrm{N} = 5b+2. \end{cases}$

a) Montrer que le couple $(a\,;\,b)$ est solution de (E).

b) Quel est le reste, dans la division de N par 40 ?

3. a) Résoudre l'équation $8x+5y=100$, où $(x\,;\,y)$ est un couple de nombres entiers relatifs.

b) Au VIII$^{\text{e}}$ siècle, un groupe composé d'hommes et de femmes a dépensé 100 pièces de monnaie dans une auberge. Les hommes ont dépensé 8 pièces chacun et les femmes 5 pièces chacune. Combien pouvait-il y avoir d'hommes et de femmes dans le groupe ?

Exercice 75

Dans tout l'exercice x et y désignent des entiers naturels non nuls vérifiant $x < y$.
S est l'ensemble des couples (x, y) tels que PGCD$(x,\ y) = y - x$.

1. a) Calculer le PGCD(363, 484).

b) Le couple (363, 484) appartient-il à S ?

2. Soit n un entier naturel non nul ; le couple $(n,\ n+1)$ appartient-il à S ?
Justifier votre réponse.

3. a) Montrer que $(x,\ y)$ appartient à S si et seulement si il existe un entier naturel k non nul tel que $x = k(y-x)$ et $y = (k+1)(y-x)$.

b) En déduire que pour tout couple $(x,\ y)$ de S on a :
PPCM $(x,\ y) = k(k+1)(y-x)$.

4. a) Déterminer l'ensemble des entiers naturels diviseurs de 228.

b) En déduire l'ensemble des couples $(x,\ y)$ de S tels que PPCM $(x,\ y) = 228$.