Feuille 1

M1 MEEF - Arithmétique

Notre objectif n'est pas seulement de réussir à produire des solutions pour les exercices suivants : nous souhaitons maîtriser leur rédaction, et prendre du recul (quand nous le pourrons, nous comparerons des solutions différentes).

Quand on ne précise pas, le terme *entier* désigne un *entier relatif*.

`Exercice 1.` Montrer que pour tout entier naturel n on a 7 qui divise $3^{2n+1} + 2^{n+2}$.

`Exercice 2.` Chercher tous les entiers n tels que $n-1$ divise $n+3$.

`Exercice 3.` Chercher tous les premiers $p > 3$ tels que 24 divise $p^2 - 1$.

`Exercice 4.` Combien de diviseurs l'entier 18! admet-il ?

`Exercice 5.` Calculer le reste de 100^{1000} dans la division euclidienne par 13.

`Exercice 6.` Montrer que pour tout entier n on a n^7 qui est congru à n modulo 42.
On essaiera d'être *efficace*.

`Exercice 7.` Déterminer l'ensemble des entiers relatifs n tels quel
1. $n+1$ divise 13
2. $n+1$ divise n^2+1
3. $n-3$ divise n^2-3.

`Exercice 8.` Montrer que pour tout entier m on a

a) $m(m+1)(m+2)(m+3)$ qui est divisible par 24 et

b) $m(m+1)(m+2)(m+3)(m+4)$ qui est divisible par 120.

`Exercice 9.`
1. Chercher tous les entiers m et n tels que $mn = 3m + 2n$.
2. Construire un exercice destiné à une classe de Terminale amenant à résoudre cette équation, de façon guidée.

`Exercice 10.`
Déterminer l'ensemble des entiers a et b tels que
1. $PGCD(a,b) = 37$ et $a + b = 296$.
2. $PGCD(a,b) = 11$ et $a + b = 111$.

`Exercice 11.` Pour tout entier relatif n calculer le PPCM de n et $n+1$.

`Exercice 12.` Quels sont les entiers a et b tels que $3^a 7^b$ finisse par un 1 en base 10 ?

`Exercice 13.` Déterminer les couples d'entiers qui ont pour pgcd 18 et pour somme 360.

`Exercice 14.` **Equations diophantiennes.**
Résoudre les équations suivantes dans $\mathbb{Z}^2$. On pourra reprendre le cours de Terminale.

$$\text{a) } 12x - 15y = 7$$
$$\text{b) } 7x + 5y = 3$$

`Exercice 15.` Démontrer que $\sqrt[3]{\frac{5}{4}}$ est irrationnel.

`Exercice 16.` Démontrer que deux entiers sont premiers entre eux si et seulement si leur somme et leur produit sont premiers entre eux.

`Exercice 17.` Montrer que pour tout $(a, b) \in \mathbb{Z}^2$ on a 7 qui divise $a^2 + b^2$ si et seulement si 7 divise a et b.

`Exercice 18.`
1. Sans utiliser les congruences, retrouver les critères de divisibilité par 2, 3, 5, 10, 9,...
2. Quel peut être l'intérêt de la question précédente ?

`Exercice 19.` Soit p un nombre premier. Résoudre l'équation $x^2 - y^2 = p$ dans $\mathbb{Z}^2$.

`Exercice 20.` Quels sont tous les entiers a et b tels que $pgcd(a, b) = a + b - 1$?

`Exercice 21.` On cherche à résoudre l'équation $x^2 = y^2 + x \wedge y + 2$ dans $\mathbb{N}^2$.
1. On suppose que deux entiers naturels x et y vérifient l'équation. Montrer que leur pgcd d vérifie $d = 1$ ou $d = 2$.
2. En déduire que $(x, y) = (2, 1)$ ou $(x, y) = (2, 0)$.
3. Conclure.
4. Quels types de raisonnement ont été utilisés dans cet exercice ?

`Exercice 22.` **Une infinité de nombres premiers.**
1. Montrer que l'ensemble des nombres premiers est infini. Un argument classique consiste à considérer $p_1 \dots p_n + 1$ où les p_i désignent...
2. Dans cette question on souhaite montrer que parmi ces nombres premiers il en existe une infinité qui soient congrus à 3 modulo 4. On note $\mathcal{T}$ l'ensemble des nombres premiers congrus à 3 modulo 4.
2.1. Montrer que $\mathcal{T}$ est non vide.
2.2. Montrer que le produit de deux entiers congrus à 1 modulo 4 reste congru à 1 modulo 4.
2.3. On suppose que $\mathcal{T}$ est fini et que $\mathcal{T} = \{p_1, p_2, \dots, p_n\}$. On note $a = 4p_1 \dots p_n - 1$. Montrer que a admet un diviseur premier congru à 3 modulo 4.
2.4 Aboutir à une contradiction et conclure.

`Exercice 23.` **Un théorème du cours très important, mais souvent malmené.**

On considère trois entiers relatifs non nuls m, n et k ainsi que les deux propositions

$$\text{a)} \quad mn \mid k \quad \text{et}$$
$$\text{b)} \quad m \mid k, n \mid k \text{ et } m \text{ premier avec } n.$$

1. Proposer un énoncé destiné à une classe de Terminale qui indique les implications éventuelles entre ces deux propositions, et qui éventuellement indique quand il n'y a pas d'implication.

2. Donner une preuve de votre énoncé destinée à une classe de Terminale ayant connaissance du cours d'arithmétique.
3. Analyser la proposition de réponse suivante :

> Montrons que b) implique a). Soit m, n et k trois entiers naturel
>
> $m \mid k$, que $n \mid k$ et que m soit premier avec n.
>
> Comme $m \mid k$ on a l'existence de $a \in \mathbb{Z}$ tel que $ma = k$.
>
> De même, comme $n \mid k$ on a l'existence de $b \in \mathbb{Z}$ tel que $nb = k$.
>
> On a donc $ma = nb$.
>
> Donc m divise nb, et donc m divise n ou b.
>
> De même, n divise ma, et donc n divise m ou a.
>
> Raisonnons par disjonction de cas : si m divise b, alors il existe $t \in \mathbb{Z}$ tel que $mt = b$, et donc $mnt = k$, d'où mn divise bien k.
>
> Dans le cas où n divise a, de la même façon il existe $t \in \mathbb{Z}$ tel que $nt = a$, et donc $mnt = k$ et on a encore mn qui divise k.
>
> Il ne reste que $m \mid n$ et $n \mid m$, ce qui implique que $m = n$ ou $m = -n$. Mais m et n sont premiers entre eux, d'où m et n ne peuvent valoir que 1 ou -1, et donc mn vaut 1 ou -1 et il divise k.

En quel énoncé faux l'étudiant semble-t-il croire ? Prouver que cet énoncé est bien faux.
4. Démontrer le lemme d'Euclide, c'est-à-dire que pour tout nombre premier p et pour deux entiers a et b, on a p qui divise ab si et seulement si p divise a ou p divise b. On proposera une démonstration rapide, en deux ou trois lignes, en utilisant un théorème du cours.
5. On considère un entier naturel $n \geq 2$. Montrer que pour tout $(a, b, m) \in \mathbb{Z}^3$ tel que m soit premier avec n, l'égalité $am \equiv bm(n)$ implique $a \equiv b(n)$.

`Exercice 24.` **Deux définitions de la congruence.**
Dans deux cours différents, on trouve les deux définitions suivantes de la notion de congruence.

> **Définition 1.** Soit a et b deux entiers relatifs et n un entier naturel tel que $n \geq 2$. On dit que a est congru à b modulo n si a et b ont même reste dans la division euclidienne par n. On note alors $a \equiv b\ (n)$.

> **Définition 2.** Soit a et b deux entiers relatifs et n un entier naturel tel que $n \geq 2$. On dit que a est congru à b modulo n si $a - b$ est un multiple de n. On note alors $a \equiv b\ (n)$.

1. Donner un énoncé du théorème de division euclidienne dans $\mathbb{Z}$.
2. Montrer que les deux définitions ci-dessus sont équivalentes.
3. Enoncer un résultat classique du cours sur les congruences, de votre choix, se démontrant facilement et naturellement à l'aide de la *Définition 2* puis le démontrer. On pourra par exemple penser aux théorèmes du cours sur les opérations algébriques.

`Exercice 25.` **Petit théorème de Fermat.**
On souhaite dans cette partie proposer une démonstration du théorème suivant :

> **Petit théorème de Fermat.** Soit a un entier naturel et p un nombre premier.
> Si p ne divise pas a, alors $a^{p-1} \equiv 1\ (p)$.

Pour la suite on considère un nombre premier p fixé.

1. Montrer que pour tout entier k compris entre 1 et $p-1$, on a p qui divise $k! \times \binom{p}{k}$.

2. Analyser cette proposition de réponse à la question précédente, et proposer une remédiation.

Par définition de

$k!\binom{p}{k} = k!\frac{p!}{k!(p-k)!} = \frac{p!}{(p-k)!}$

d'où $p\frac{(p-1)!}{(p-k)!} = k!\binom{p}{k}$ et donc p divise $k!\binom{p}{k}$

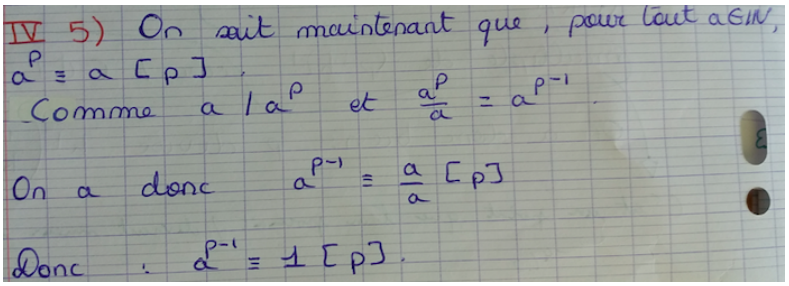
3. En déduire que pour tout entier k compris entre 1 et $p-1$ on a p qui divise $\binom{p}{k}$.

4. A l'aide du binôme de Newton, montrer que pour tout entier naturel a on a $(a+1)^p \equiv a^p + 1\ (p)$.

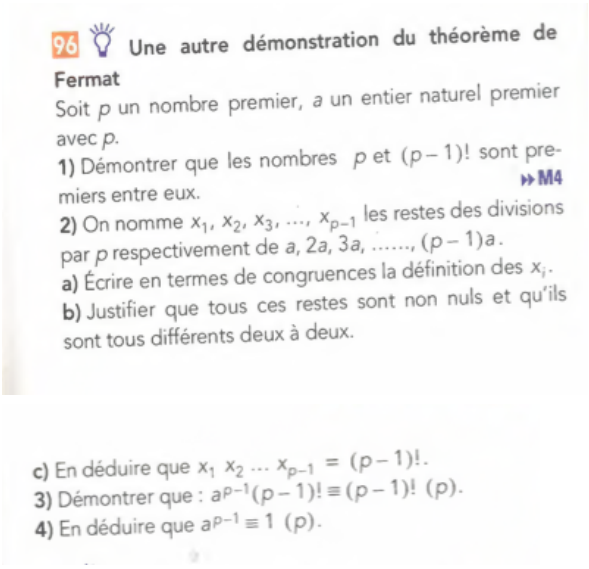
5. En déduire que pour tout entier naturel a on a $a^p \equiv a\ (p)$.

6. Conclure.

7. Analyser la proposition de réponse suivante à la question **6.**


IV 5) On sait maintenant que, pour tout $a \in \mathbb{N}$, $a^p \equiv a\ [p]$.
Comme $a \mid a^p$ et $\frac{a^p}{a} = a^{p-1}$.
On a donc $a^{p-1} \equiv \frac{a}{a}\ [p]$
Donc : $a^{p-1} \equiv 1\ [p]$.

8. Dans cette question on s'intéresse à une autre preuve de ce théorème, celle proposée dans l'exercice suivant.


96 **Une autre démonstration du théorème de Fermat**

Soit p un nombre premier, a un entier naturel premier avec p.

1) Démontrer que les nombres p et $(p-1)!$ sont premiers entre eux. ▸▸M4

2) On nomme $x_1, x_2, x_3, \ldots, x_{p-1}$ les restes des divisions par p respectivement de $a, 2a, 3a, \ldots\ldots, (p-1)a$.

a) Écrire en termes de congruences la définition des x_i.

b) Justifier que tous ces restes sont non nuls et qu'ils sont tous différents deux à deux.

c) En déduire que $x_1\ x_2 \ldots x_{p-1} = (p-1)!$.

3) Démontrer que : $a^{p-1}(p-1)! \equiv (p-1)!\ (p)$.

4) En déduire que $a^{p-1} \equiv 1\ (p)$.

8.a. Dans cette sous-question, on souhaite prendre du recul par rapport à la question **2)b)** . Pour cela, on considère la fonction ϕ_a : $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ qui à la classe de t associe la classe de $a.t$. Reformuler sans explication la question **2)b)** en terme d'une propriété de cette fonction ϕ_a. (On ne demande pas de corriger la question **2)b))** .
8.b. Proposer une correction de la question **4)** à partir de la question **3)** qui soit destinée à une classe de Terminale.

Jusqu'à la fin de l'exercice, on souhaite prendre du recul avec nos connaissances du supérieur.

9. On considère un entier $n \geq 2$. On suppose connue la structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$, et on souhaite montrer dans les questions suivantes que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
9.a. Montrer que si n n'est pas premier, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre, c'est-à-dire qu'il existe deux éléments différents de $\overline{0}$ dont le produit égale $\overline{0}$.
9.b Montrer que si n est premier, alors $\mathbb{Z}/n\mathbb{Z}$ est un corps. On pourra utiliser la relation de Bézout.
9.c Conclure.

`Exercice 26.` *Un petit défi.* On définit quatre entiers A, B, C et D ainsi : $A = 4444^{4444}$, B est la somme des chiffres de A, C est la somme des chiffres de B et D est la somme des chiffres de C. Calculer D.

`Exercice 27.` L'objectif de cet exercice est de trouver tous les couples d'entiers (a, b) tels que $a^b = b^a$.
1. Montrer que pour tout entier $n \geq 3$ on a $2^{n-1} > n$.
2. Montrer que si deux entiers u et v sont premiers entre eux, alors pour tout entier n on a u et v^n qui sont premiers entre eux également.
3. Dans cette questions **3.** on considère un couple d'entiers (a, b) solution du problème et tel que $0 < a < b$. On note d le pgcd de a et de b, et on considère des entiers a' et b' tels que $a = da'$ et $b = db'$.
3.a Montrer que $d = a$ et que $d^{d(b'-1)} = b'^d$.
3.b Traiter les cas $d = 1$, $d = 2$ et $d \geq 3$.
4. Conclure.
5. Proposer une autre solution de l'exercice basée sur l'étude de la fonction $x \mapsto \ln(x)/x$.

`Exercice 28.` L'objectif de cet exercice est prouver un point important du cours : la terminaison et la validité de l'algorithme d'Euclide.
1. Proposer une version simple de l'algorithme d'Euclide (on pourra décrire cet algorithme en *pseudocode*).
2. Démontrer que toute suite d'entiers positifs strictement décroissante est finie.
3. En considérant la suite des restes calculés à chaque étape, montrer que l'algorithme **termine**. (Remarquer qu'une des difficultés est de définir proprement cette suite des restes !)
4. On considère deux entiers naturels a et b, avec b non nul. On note r le reste dans la division euclidienne de a par b. Montrer que $pgcd(a, b) = pgcd(b, r)$.
5. Montrer **la validité** de l'algorithme d'Euclide, c'est-à-dire qu'il renvoie bien le résultat souhaité.