

CPGE My Youssef, Rabat



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ
وَ قُلْ إِعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَ رَسُولُهُ وَ
الْمُؤْمِنُونَ

صَدَقَ اللَّهُ الْعَظِيمِ

Feuille d'exercices: *Arithmétique*

28 février 2009

Blagues du jour :

- Si les cons étaient des fleurs, la salle des profs de maths serait un jardin...
- Qu'est-ce qu'un bon professeur ? Un bon professeur c'est un prof qui est absent.
- L'inspecteur demande à un professeur : "Pouvez-vous me donner 2 raisons qui vous motivent à devenir professeur ?", juillet et août, lui répondit.
- Un professeur de médecine à ses étudiants : Qui provoque la transpiration, vos questions, monsieur ; lui répondent.

Mathématicien du jour

Euclide
Euclide(-325 Av. JC- -265 Av. JC) est un mathématicien de la Grèce antique, auteur des *Éléments*, qui sont considérés comme l'un des textes fondateurs des mathématiques modernes. Il partit en Égypte pour y enseigner les mathématiques et fût contemporain d'Archimède.

Les *Éléments* sont une compilation du savoir géométrique et restèrent le noyau de l'enseignement mathématique pendant près de 2000 ans. Il se peut qu'aucun des résultats contenus dans les *Éléments* ne soit d'Euclide, mais l'organisation de la matière et son exposé lui sont dus.



Exercice 1 . Montrer les propriétés suivantes :

- 1) $\forall (a, b, c) \in \mathbb{N}^3 : (9 \text{ divise } a^3 + b^3 + c^3) \Rightarrow (3 \text{ divise } a \text{ ou } b \text{ ou } c)$
- 2) $\forall (a, b, c) \in \mathbb{N}^3 : (7 \text{ divise } a^3 + b^3 + c^3) \Rightarrow (7 \text{ divise } abc)$
- 3) $\forall n \in \mathbb{N}$ on a : 6 divise $5n^3 + n$
- 4) $\forall n \in \mathbb{N}$ on a : 9 divise $n^3 + (n+1)^3 + (n+2)^3$

Exercice 2 . Donner le chiffres des unités de 4444^{4444} .

Indication : On pourra travailler dans $\mathbb{Z}/10\mathbb{Z}$.

Exercice 3 . On pose $N = 4444^{4444}$, A la somme des chiffres de N , B celle de A et enfin C celle de B . Trouver C .

Indication : On pourra utiliser qu'un nombre n et la somme de ses chiffres $\varphi(n)$ sont toujours congrus modulo 9, et que si $n < 10^k$, alors $\varphi(n) \leq 9k$

Exercice 4 . Soit $N = 111111111$, écrit en base 10. Justifier que : $N^2 = 12345678987654321$

Exercice 5 .

- 1) Nous sommes le mercredi 4 Mars 2009, l'année prochaine quel jour sera le 4 Mars 2010 ?
- 2) Dans quelle année le 4 Mars sera un mercredi ?

Exercice 6 . Trouver tous les chiffres x et y tels que le chiffre suivant écrit en base 10, $28x75y$ soit divisible par 3 et par 11.

Exercice 7 . Soit $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$, montrer que : $a \wedge b = 1 \Leftrightarrow ab \wedge (a + b) = 1$.

Exercice 8 . Résoudre dans $\mathbb{N}^* \times \mathbb{N}^*$ le système suivant :
$$\begin{cases} x \geq y \\ x \vee y = (x \wedge y)^2 \\ x \vee y + x \wedge y = 156 \end{cases}$$

Exercice 9 . Soit $n \in \mathbb{N}$, on pose $x = 3n + 1, y = 5n - 1$.

- 1) Montrer que $x \wedge y$ divise 8.
- 2) Trouver les entiers n tels que $x \wedge y = 8$.

Exercice 10 . Soit $n \in \mathbb{N}$. Montrer que : 2^n divise $(3 + \sqrt{5})^n + (3 - \sqrt{5})^n$.

Exercice 11 . Soient $a, b \in \mathbb{N}^*$ premiers entre eux tels que ab est un carré parfait. Montrer que a et b sont des carrés parfaits.

Exercice 12 . Soient $a, b \in \mathbb{N}^*$ et m, n premiers entre eux tels que $a^n = b^m$. Montrer qu'il existe $c \in \mathbb{N}^*$ tel que $a = c^m$ et $b = c^n$.

Exercice 13 . Soient $a \in \mathbb{N}, a \geq 2, (m, n) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $m \geq n$. On pose $m = qn + r$ avec $0 \leq r < n$.

- 1) Montrer que : $\exists b \in \mathbb{N}; a^m - 1 = (a^n - 1)b + a^r - 1$.
- 2) Montrer que : $(a^m - 1) \wedge (a^n - 1) = a^{m \wedge n} - 1$.
- 3) Montrer que : $(a^n - 1)$ divise $(a^m - 1) \Leftrightarrow n$ divise m
- 4) *Application* : Soit N_k le nombre qui s'écrit en base 10 avec k chiffres tous égaux à 1. Montrer que : N_h divise $N_k \Leftrightarrow h$ divise k .

Exercice 14 . *Nombres de Fermat.*

Les nombres de Fermat sont ceux de la forme : $F_n = 2^{2^n} + 1$

- 1) Montrer que tous ces nombres sont premiers entre eux deux à deux
- 2) Montrer que F_n est premier pour $n \in [0, 4]$ mais F_5 ne l'est pas
- 3) Soit $a \in \mathbb{N}^*$ montrer que si $2^a + 1$ est premier alors a est une puissance de 2

A l'heure actuelle on ne connaît pas nombre de Fermat premier autre que F_n où $n \in [0, 4]$, mais on connaît plusieurs qui ne le sont pas : F_{1945} qui a plus de 10582 chiffres est divisible par $2^{1947}5 + 1$ qui a exactement 587 chiffres.

Exercice 15 . *Décomposition à coefficients positifs.*

Soient $a, b \in \mathbb{N}^*$ premiers entre eux. Montrer que : $\forall x \geq ab, \exists u, v \in \mathbb{N}$ tels que $au + bv = x$.

Exercice 16 . *Crible d'Erathostène.*

- 1) Montrer que tout entier supérieur à 2 non premier admet au moins un diviseur premier inférieur à sa racine.
- 2) Énoncer le *crible d'Erathostène* qui permet de tester si un nombre est premier.
- 3) Donner les 20 premiers nombres premiers
- 4) Les nombres suivants sont - ils premiers : 353 , 91451

Exercice 17 . Critère d'Eseinstein

- 1) Soient $(p, q) \in \mathbb{Z} \times \mathbb{N}$ tel que $p \wedge q = 1$ et $(a_i)_{0 \leq i \leq n} \in \mathbb{N}^{n+1}$.
Montrer que si $\frac{p}{q} \in \mathbb{Q}$ est solution de l'équation : $a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 = 0$,
alors : p divise a_0 et q divise a_n
- 2) Résoudre l'équation : $30X^3 - 37X^2 + 15X - 2 = 0$

Exercice 18 . Nombres de Mersenne.

Ils sont de la forme : $M_p = 2^p - 1$ avec p premier.

- 1) Montrer que les Nombres de Mersenne sont premiers entre eux deux à deux.
- 2) Soit $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que : $a^b - 1$ est premier, montrer alors que : $a = 2$ et b premier.

Le plus grand nombre premier découvert jusqu'à nos jours est un nombre de Mersenne. C'est $2^{43,112,609} - 1$; le 45 ème nombre de Mersenne premier découvert le 23 Août 2008, par un américain (Edson Smith). La méthode utilisé s'appelle GIMPS (Great Internet Mersenne Prime Search), qui consiste à utiliser plusieurs serveurs distants connectés via internet.

Exercice 19 . Théorème de Wilson.

Soit p un entier premier.

- 1) Montrer que $\forall \bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, $\exists \bar{b} \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $\bar{a}\bar{b} = \bar{1}$.
- 2) En déduire que : $(p-1)! \equiv -1 \pmod{p}$.

Exercice 20 . Cryptographie-RSA

Soit p et q deux nombres premiers, on pose $n = pq$. Soit M un entier naturel premier avec pq , qui représente le message à décoder, et C le message codé envoyé.

- 1) Dites pourquoi $\varphi(n) = (p-1)(q-1)$.
- 2) Soit e premier avec $\varphi(n)$, justifier l'existence de $d \in \mathbb{Z}$ tel que $ed \equiv 1 \pmod{\varphi(n)}$.
- 3) Le message M est codé en C tel que $C \equiv M^e \pmod{n}$.
En déduire que : $C^d \equiv M \pmod{n}$.

Indication : On pourra penser à utiliser le théorème d'Euler.

Remarques : Rivest Shamir Adleman ou RSA est un algorithme asymétrique de cryptographie à clé publique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme a été décrit en 1977 par Ron Rivest, Adi Shamir et Len Adleman, d'où le sigle RSA. En 2008, c'est le système à clef publique le plus utilisé (carte bancaire française, de nombreux sites web commerciaux, ...).

Le couple (n, e) est appelé clef publique alors que le couple (n, d) est appelé clef privée. On constate que pour chiffrer un message, il suffit de connaître e et n . En revanche pour déchiffrer, il faut d et n . Ainsi il suffit de connaître p, q et e puisque $\varphi(n) = (p-1)(q-1)$ et $d \equiv e^{-1} \pmod{\varphi(n)}$.

Exercice 21 . Petit Théorème de Fermat.

Soit p un nombre premier.

1) Montrer que p divise $\binom{p}{k}$, $\forall k \in [1, p-1]$.

Indication : Utiliser le théorème de Gauss.

2) Montrer que pour tous $n, m \in \mathbb{N}^2$ on a : $(n + m)^p \equiv n^p + m^p \pmod{p}$

3) Que peut-on dire alors de l'application $\phi : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$.
 $\bar{x} \mapsto \bar{x}^p$

4) Montrer que : $\forall n \in \mathbb{N} : n^p \equiv n \pmod{p}$.

Exercice 22 . Problème de Bezout.

Soient a, b, c trois entiers relatifs. On considère l'équation : $ax + by = c$, appelée problème de Bezout dont on recherche les solutions dans \mathbb{Z}^2 .

1) Donner une condition nécessaire et suffisante pour que cette équation admette une solution.

2) Soit (x_0, y_0) une solution particulière du problème de Bézout. Déterminer la forme générale des autres solutions (x, y) en fonction de $a, b, d = a \wedge b, x_0$ et y_0 .

3) Résoudre dans \mathbb{Z}^2 :

a) $95x + 71y = 46$.

b) $20x - 53y = 3$.

c) $12x + 15y + 20z = 7$.

d) $2520x - 3960y = 6480$.

Exercice 23 . Congruences simultanées, théorème des restes chinois.

Soient $a, b, n, m \in \mathbb{Z}$ avec $n \wedge m = 1$.

On considère le système : $\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases} \quad (S)$

1) Justifier l'existence de $(u, v) \in \mathbb{N}^2$, tel que $\begin{cases} nu \equiv 1 \pmod{m} \\ mv \equiv 1 \pmod{n} \end{cases}$.

2) En déduire que $x_0 = amv + bnu$ est une solution particulière du système (S) .

3) Montrer que toutes les autres solutions sont congrues avec x_0 modulo nm .

4) Résoudre : $\begin{cases} x \equiv 2 \pmod{140} \\ x \equiv -3 \pmod{99} \end{cases}$

5) *Application.*

Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces.

Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces.

Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces.

Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

Réponse : 785

*Fin
à la prochaine*