Arithmétique

Mercredi 1 Février 2017

Al-Samawal Al Maghribi (1220-1283)

Savant marocain et fils de rabbin, est connu pour ses ouvrages qui traitent la trigonométrie. En effet, il était parmi les pionniers de cette discipline : il avait révélé dans ses écrits, les méthodes pour calculer l'aire des triangles, cercles, carrés ainsi que d'autres formes géométriques. Il est le premier à avoir utilisé le raisonnement par récurrence.

Blague du jour

Bonjour, vous avez rejoint la messagerie vocale d'aide psychiatrique.

- Si vous êtes dépressif, le numéro sur lequel vous appuierez est sans importance, personne ne répondra.
- Si vous êtes un compulsif a répétition, raccrochez et recomposez.
- Si vous êtes un agressif-passif, mettez-nous en attente.
- Si vous êtes antisocial, arrachez le téléphone du mur.
- Si vous avez des difficultés d'attention, ne vous occupez pas des instructions.

Exercice 1

Montrer les propriétés suivantes :

1. $\forall (a,b,c) \in \mathbb{N}^3$: (9 divise $a^3+b^3+c^3$) $\Rightarrow$ (3 divise a ou b ou c)
2. $\forall (a,b,c) \in \mathbb{N}^3$: (7 divise $a^3+b^3+c^3$) $\Rightarrow$ (7 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* $\varphi(n) \leqslant 9k$

Exercice 4

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

Exercice 5

1. Nous sommes le mercredi 1 Février 2017, l'année prochaine quel jour sera le 1 Février 2018 ?
2. Dans quelle année le 1 Février sera un mercredi ?

Exercice 6

Trouver tous les chiffres x et y tels que le chiffre suivant s'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 systéme 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 $\left(3+\sqrt{5}\right)^n + \left(3-\sqrt{5}\right)^n$.

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 $a, b, m, n \in \mathbb{N}^*$ tq $m \wedge n = 1$ et $a^n = b^m$. Montrer que $\exists c \in \mathbb{N}^*$ tel que $a = c^m, b = c^n$.

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 $(a^m - 1) \Longleftrightarrow n$ divise m
4. *Application* : Soit N_k le nombre qui s'écrit en base 10 avec k chiffres tous égaux 1. Montrer que : N_h divise $N_k \Longleftrightarrow h$ divise k.

Exercice 14 : Nombres de Fermat ($F_n = 2^{2^n} + 1$)

1. Montrer que tous ces nombres sont premiers entre eux deux 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 connait pas nombre de Fermat premier autre que F_n o $n \in [|0, 4|]$, mais on connait 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 : $\forall\, x \geqslant ab$, $\exists\, u, v \in \mathbb{N}$ tels que $au + bv = x$.

Exercice 16 : Crible d'Eratosthène.

1. Montrer que tout entier supérieur 2 non premier admet au moins un diviseur premier inférieur sa racine.
2. Énoncer le *crible d'Erathostne* 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'ééquation : $a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 = 0$, alors : p divise a_0 et q divise a_n
2. Résoudre l'ééquation : $30X^3 - 37X^2 + 15X - 2 = 0$

Exercice 18 : Nombres de Mersenne ($M_p = 2^p - 1$ avec p premier.)

1. Montrer que les *Nombres de Mersenne* sont premiers entre eux deux 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.

Exercice 19 : Théorème de Wilson

Soit p un entier premier.

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

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 : $C^d \equiv M \pmod{n}$.

RSA

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

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

Exercice 21 : Petit Théorème de Fermat.

Soit p un nombre premier.

1. Montrer que p divise $\binom{p}{k}$, $\quad \forall k \in [\![1, p-1]\!]$. *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 $\begin{array}{rccc} \phi :: & \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ & \overline{x} & \mapsto & \overline{x}^p \end{array}$.
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 $\mathbb{Z}^2$: $95x + 71y = 46$.

Exercice 23 : 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 tus. 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 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