Classe de TS

Démonstrations à connaître — Arithmétique

Restitution organisée des connaissances

Pour chaque question nous rappelons la démonstration et nous essayons de proposer une mise en situation… Lorsqu'il n'y a pas de démonstartion demandée vous pouvez inventer une question…

Spécialité : arithmétique

Spécialité : arithmétique

1-a : Théorème de la division euclidienne

Soient a un entier relatif et b un entier non nul ; il existe un couple d'entiers relatifs (q, r) tels que

$$a = bq + r \text{ avec } 0 \le r < b .$$

L'opération qui au couple (a, b) associe le couple (q, r) est appelée *division euclidienne*. q est le *quotient*, r le *reste*.

Démonstration : soit x un réel, on appelle *partie entière* de x le nombre entier relatif juste inférieur à x ; on le note E(x). La division de a par b fournit un nombre réel $u = \frac{a}{b}$; soit alors $q = \text{E}(u)$, on a alors

$$q \le \frac{a}{b} < q + 1 \Leftrightarrow qb \le a < qb + b \Leftrightarrow 0 \le a - qb < b .$$

Posons $r = a - qb$, on a évidemment $a = qb + r$ et $0 \le r < b$. L'existence de r est assurée, celle de q est due à l'existence d'un entier égal à la partie entière d'un réel, chose que nous admettrons…

S'il existait deux couples (q, r) et (q', r') on aurait de la même manière $a = bq + r = bq' + r'$ d'où $b(q - q') = r - r'$ donc $r - r'$ est un multiple de b, mais on a $-b < r - r' < b$, la seule possibilité est donc que $r - r' = 0 \Leftrightarrow r = r'$ et comme b n'est pas nul, que $q - q' = 0$, soit $q = q'$. Nous avons donc unicité.

Exercice

n désigne un nombre entier naturel.

1. Démontrer que $n^2 + 5n + 4$ et $n^2 + 3n + 2$ sont divisibles par $n + 1$.

2. Déterminer l'ensemble des entiers n pour lesquels $3n^2 + 15n + 19$ est divisible par $n + 1$.

3. En déduire que, quel que soit n, $3n^2 + 15n + 19$ n'est pas divisible par $n^2 + 3n + 2$.

Peut-on préciser, suivant les valeurs de n, le reste de la division de $3n^2 + 15n + 19$ par $n^2 + 3n + 2$?

1-b : Algorithme d'Euclide

Ecrivons les divisions successives de a par b, de r_0 par r_1, … jusqu'à celle de r_{n-1} par r_n :

$$a = bq_0 + r_0$$
$$b = r_0 q_1 + r_1$$
$$r_0 = r_1 q_2 + r_2$$
....
$$r_{n-1} = r_n q_{n+1} + r_{n+1}$$

Comme on a $0 \le r_{n+1} < r_n < ... < r_1 < r_0 < b$ et que ce sont tous des nombre entiers, il arrivera forcément un moment où r_{n+1} sera nul (principe de la *descente infinie* de Fermat) sinon on aboutirait à une contradiction.

Supposons par exemple que r_N soit le dernier reste non nul ; on a $r_0 = a - bq_0$ et si d est un diviseur de a et b, d divise alors $a - bq_0$ et donc r_0, d est un diviseur de b et r_0. Le même raisonnement appliqué aux divisions successives montre que d est un diviseur de a, b, r_0, r_1, …, r_N.

Particulièrement, si d est le Plus Grand Commun Diviseur de a et b, c'est également celui de b et r_0, de r_0 et r_1, de r_1 et r_2,…de r_{N-1} et r_N. Or on a $r_{N-1} = q_{N+1} r_N$ donc r_N divise r_{N-1}, c'est le PGCD de a et b.

Exercice 1

1. Démontrer que, pour tout entier naturel n, $2^{3n} - 1$ est un multiple de 7. En déduire que $2^{3n+1} - 2$ et $2^{3n+2} - 4$ sont des multiples de 7.

2. Déterminer les restes de la division par 7 des puissances de 2.

3. Soit p un entier et le nombre $A_p = 2^p + 2^{2p} + 2^{3p}$. Déterminer suivant que $p = 3n$, $3n+1$ ou $3n+2$ la divisibilité de A_p par 7.

Exercice 2

On considère les entiers naturels a, b et c qui s'écrivent dans la base n : $a = 111$, $b = 114$ et $c = 13054$.

1. Sachant que $c = ab$, déterminer n puis l'écriture de chacun de ces nombres en base 10.

2. Vérifier, en utilisant l'algorithme d'Euclide, que a et b sont premiers entre eux. En déduire les solutions dans $\mathbb{Z}^2$ de l'équation $ax + by = 1$.

1-c : Propriétés de la congruence

Si $a \equiv p(n)$ et $b \equiv q(n)$ alors

$a \pm b \equiv (p \pm q)(n)$: par exemple on a $a = p + kn$, $b = q + k'n$ d'où $a + b = p + q + (k + k')n \Leftrightarrow a + b \equiv p + q(n)$;

$ab \equiv pq(n)$: $a = p + kn$, $b = q + k'n$, d'où $ab = (p + kn)(q + k'n) = pq + kqn + k'pn + kk'qpn^2 \Rightarrow ab \equiv pq(n)$;

on en déduit immédiatement que $a^m \equiv p^m(n)$ par récurrence sur m.

Exercice

On considère les dix caractères A, B, C, D, E, F, G, H, I et J auxquels on associe dans l'ordre les nombres entiers de 1 à 10. On note $\Omega = \{1, 2, \ldots, 10\}$.

Définition de la congruence modulo 11 : on rappelle que si a et b désignent deux entiers relatifs, on dit que a est congru à b modulo 11, et on écrit $a \equiv b[11]$, si et seulement s'il existe un entier relatif k tel que $a = b + 11k$.

1. a. **Démonstration de cours** : démontrer que si $a \equiv b[11]$ et $c \equiv d[11]$ alors $ac \equiv bd[11]$.

b. En déduire que si $a \equiv b[11]$, alors pour tout n entier naturel on a : $a^n \equiv b^n[11]$.

2. On désigne par f la fonction définie sur Ω par « $f(n)$ est le reste de la division euclidienne de 5^n par 11 ».

On désire coder à l'aide de f le message « BACF ». Compléter la grille de chiffrement ci-dessous :

Lettre	B	A	C	F
n	2	1	3	6
$f(n)$	3			
Lettre	C			

Peut-on déchiffrer le message codé sans ambiguïté ?

3. On désigne par g la fonction définie sur Ω par « $g(n)$ est le reste de la division euclidienne de 2^n par 11 ». Etablir, sur le modèle précédent, la grille de chiffrement de g. Permet-elle le déchiffrement sans ambiguïté de tout message codé à l'aide de g ?

4. Le but de cette question est de déterminer des conditions sur l'entier a compris entre 1 et 10 pour que la fonction h définie sur E par « $h(n)$ est le reste de la division euclidienne de a^n par 11 » permette de chiffrer et déchiffrer correctement un message de 10 caractères.

Soit i un élément de Ω.

a. Montrer, en raisonnant par l'absurde, que si, pour tout $i \in \Omega$, $i < 10$, a^i n'est pas congru à 1 modulo 11, alors la fonction h permet le déchiffrement sans ambiguïté de tous messages.

b. Montrer que s'il existe $i \in \Omega$, $i < 10$, tel que $a^i \equiv 1[11]$, alors la fonction h ne permet pas de déchiffrer un message avec certitude.

c. On suppose que i est le plus petit entier naturel tel que $1 \le i \le 10$ vérifiant $a^i \equiv 1[11]$.

En utilisant la division euclidienne de 10 par i, prouver que i est un diviseur de 10.

d. Quelle condition doit vérifier le nombre a pour permettre le chiffrage et le déchiffrage sans ambiguïté de tous messages à l'aide de la fonction h ? Faire la liste de ces nombres.

1-d : Théorème de Bézout

Soit a et b deux entiers non nuls, d leur PGCD.

Alors il existe deux entiers relatifs u et v tels que $au + bv = d$.

Démonstration : On appelle U l'ensemble des entiers **non nuls** de la forme $n = au + bv$: U n'est pas vide puisqu'il contient a, b, etc. U a alors un plus petit élément d_0 tel que $au_0 + bv_0 = d_0$; comme d divise a et b, il divise d_0 et donc $d \le d_0$.

Montrons que d peut s'écrire $au + bv = d$: on divise a par d_0, soit

$$a = d_0 q + r \Leftrightarrow r = a - d_0 q = a - (au_0 + bv_0)q = a(1 - qu_0) + b(-qv_0) \text{ avec } 0 \le r < d_0 .$$

r est donc dans U mais d_0 est le plus petit élément de U donc r est nul (sinon il serait dans U) ; conclusion d_0 divise a ; le même raisonnement avec b fait que d_0 divise b donc d_0 divise d et $d_0 \le d$. Finalement $d_0 = d$.

Remarque : cette relation permet de montrer deux choses vraiment importantes :

* a et b sont premiers entre eux si et seulement si il existe u et v entiers relatifs tels que $au + bv = 1$.

* L'équation $ax + by = c$ a des solutions en nombres entiers si et seulement si c est un multiple de d, PGCD de a et b.

Exercice 1

1. Calculer, en fonction de n, la somme des n premiers entiers naturels non nuls.

2. Démontrer par récurrence que $\sum_{p=1}^{n} p^3 = \left(\sum_{p=1}^{n} p \right)^2$. Exprimer $s_n = \sum_{p=1}^{n} p^3$ en fonction de n.

3. Soit D_n le PGCD des nombres s_n et s_{n+1} .Calculer D_n lorsque

a. $n = 2k$.

b. $n = 2k+1$.

En déduire que s_n , s_{n+1} et s_{n+2} sont premiers entre eux.

Exercice 2

Pour tout entier naturel n, non nul, on considère les nombres

$$a_n = 4\times10^n - 1\ ,\ b_n = 2\times10^n - 1 \text{ et } c_n = 2\times10^n + 1\ .$$

1. a. Calculer a_1, b_1, c_1, a_2, b_2, c_2, a_3, b_3 et c_3.

b. Combien les écritures décimales des nombres a_n et c_n ont-elles de chiffres ? Montrer que a_n et c_n sont divisibles par 3.

c. Montrer, en utilisant la liste des nombres premiers inférieurs à 100 donnée ci-dessous, que b_3 est premier.

d. Montrer que pour tout entier naturel non nul n, $b_n \times c_n = a_{2n}$.

e. Montrer que $\text{PGCD}(b_n , c_n) = \text{PGCD}(c_n , 2)$. En déduire que b_n et c_n sont premiers entre eux.

2. On considère l'équation (E) : $b_3 x + c_3 y = 1$ d'inconnues les entiers relatifs x et y.

a. Justifier le fait que (E) a au moins une solution.

b. Appliquer l'algorithme d'Euclide aux nombres c_3 et b_3 ; en déduire une solution particulière de (E).

c. Résoudre l'équation (E).

Liste des nombres premiers inférieurs à 100 : 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; 41 ; 43 ; 47 ; 53 ; 59 ; 61 ; 67 ; 71 ; 73 ; 79 ; 83 ; 89 ; 97.

Exercice 3, Nouvelle Calédonie, remplacement, novembre 2004 (c)

Dans cet exercice a et b désignent des entiers strictement positifs.

1. a. Démontrer que s'il existe deux entiers relatifs u et v tels que $au + bv = 1$ alors les nombres a et b sont premiers entre eux.

b. En déduire que si $\left(a^2 + ab - b^2 \right)^2 = 1$ alors a et b sont premiers entre eux.

2. On se propose de déterminer tous les couples d'entiers strictement positifs $(a\ ;\ b)$ tels que $\left(a^2 + ab - b^2 \right)^2 = 1$. Un tel couple sera appelé solution.

a. Déterminer a lorsque $a = b$.

b. Vérifier que (1 ; 1), (2 ; 3) et (5 ; 8) sont trois solutions particulières.

c. Montrer que si $(a\ ;\ b)$ est solution et si $a < b$, alors $a^2 - b^2 < 0$.

3. a. Montrer que si $(x\ ;\ y)$ est une solution différente de (1 ; 1) alors $(y - x\ ;\ x)$ et $(y\ ;\ y + x)$ sont aussi des solutions.

b. Déduire de 2. b. trois nouvelles solutions.

4. On considère la suite de nombres entiers strictement positifs $(a_n)_{n\in\mathbb{N}}$ définie par $a_0 = a_1 = 1$ et pour tout entier n, $n \geq 0$, $a_{n+2} = a_{n+1} + a_n$.

Démontrer que pour tout entier naturel $n \geq 0$, $(a_n\ ;\ a_{n+1})$ est solution. En déduire que les nombres a_n et a_{n+1} sont premiers entre eux.

Correction

1. a. Démonstration de cours : voir plus haut.

b. $\left(a^2+ab-b^2\right)^2=1 \Leftrightarrow \begin{cases} a^2+ab-b^2=1 \\ a^2+ab-b^2=-1 \end{cases} \Leftrightarrow \begin{cases} a(a+b)-b\times b=1 \\ b(b-a)-a\times a=1 \end{cases}$. Dans les deux cas on peut écrire $au+bv=1$: dans le premier $u=a+v, v=-b$, dans le second $u=b-a, v=-a$.

2. a. $a=b$: $\left(a^2+ab-b^2\right)^2=1 \Leftrightarrow a^4=1 \Rightarrow a=1 \ (a>0)$.

b. (1 ; 1) est déjà fait, (2 ; 3) : $\left(2^2+2.3-3^2\right)^2=1$ et (5 ; 8) : $\left(5^2+5.8-8^2\right)^2=(25+40-64)^2=1$.

c. $a^2+ab-b^2=1$: si on a $a^2-b^2>0$, alors a^2+ab-b^2 ne peut pas valoir 1 ; de même a^2+ab-b^2 ne peut valoir -1 dans ce cas puisqu'il serait positif. Dans tous les cas on a $a^2-b^2<0$.

3. a. $(y-x\,;x)$ est une solution ssi $(x\,;y)$ est une solution :

$\left((y-x)^2+(y-x)x-x^2\right)^2=\left(y^2-2xy+x^2+xy-x^2-x^2\right)^2=\left(y^2-xy+x^2\right)^2=1$;

Même calcul pour $(y\,;y+x)$.

b. (2 ; 3) est solution donc $(3-2\,;2)=(1\,;2)$ et $(3\,;3+2)=(3\,;5)$ en sont ; (5 ; 8) est solution donc $(8-5\,;5)=(3\,;5)$ et $(8\,;5+8)=(8\,;13)$ en sont ; on a les nouvelles solutions : $(1\,;2)$, $(3\,;5)$ et $(8\,;13)$.

4. $a_0=a_1=1$, $a_{n+2}=a_{n+1}+a_n$. Démonstration par récurrence : supposons que $(a_n\,;a_{n+1})$ est solution, alors $(y\,;y+x)=(a_{n+1}\,;a_n+a_{n+1})=(a_{n+1}\,;a_{n+2})$ est solution d'après le 3. a. Comme c'est vrai au rang 0 : (1 ; 1) est solution, c'est toujours vrai.

La question 1. b. justifie alors que les nombres a_n et a_{n+1} sont premiers entre eux.

1-e : Théorème de Gauss

a, *b*, *c* trois entiers non nuls ; si *a* et *b* sont premiers entre eux et que *a* divise *bc*, alors *a* divise *c*.

La démonstration est immédiate : *a* divise *bc* donc $bc=ka$, *a* et *b* sont premiers entre eux donc il existe *u* et *v* tels que $au+bv=1$, soit en multipliant par *c* : $cau+cbv=c \Rightarrow cau+kav=c \Leftrightarrow a(cu+kv)=c$; il est donc clair que *a* divise *c* (ainsi que $cu+kv$ …).

Exercice

1. On admet que 1999 est un nombre premier. Déterminer l'ensemble des couples (a, b) d'entiers naturels tels que $a + b = 11994$ et dont le PGCD vaut 1999.

2. On considère l'équation (E) : $n^2-Sn+11994=0$ où *S* est un entier naturel. On s'intéresse à des valeurs de *S* telles que (E) admette deux solutions dans $\mathbb{Z}$

a. Peut on trouver *S* tel que 3 soit solution de (E) ? Si oui, préciser la deuxième solution.

b. Même question avec 5 ?

c. Montrer que tout entier *n* solution de (E) est un diviseur de 11994. En déduire toutes les valeurs possibles de *S*.

1-f : L'ensemble des nombres premiers est infini

Il existe plus de 600 démonstrations, la plus connue restant celle d'Euclide : je ne résiste pas au plasir de vous laisser traduire la page d'Eric Weisstein : http://mathworld.wolfram.com/EuclidsTheorems.html

Euclid's second theorem states that the number of primes is infinite. This theorem, also called the infinitude of primes theorem, was proved by Euclid in Proposition IX.20 of the *Elements* (Tietze 1965, pp. 7-9). Ribenboim (1989) gives nine (and a half) proofs of this theorem. Euclid's elegant proof proceeds as follows.

Given a finite sequence of consecutive primes 2, 3, 5, ..., p, the number $N = 2.3.5....p + 1$, known as the ith Euclid number when $p = p_i$ is the ith prime, is either a new prime or the product of primes. If N is a prime, then it must be greater than the previous primes, since one plus the product of primes must be greater than each prime composing the product. Now, if N is a product of primes, then at least one of the primes must be greater than p. This can be shown as follows.

If N is composite and has no prime factors greater than p, then one of its factors (say F) must be one of the primes in the sequence, 2, 3, 5, ..., p. It therefore divides the product $2.3.5...p$. However, since it is a factor of N, it also divides N. But a number which divides two numbers a and $b < a$ also divides their difference $a - b$, so F must also divide $N - (2.3.5...p) = (2.3.5...p) + 1 - (2.3.5...p) = 1$.

However, in order to divide 1, F must be 1, which is contrary to the assumption that it is a prime in the sequence 2, 3, 5, ... It therefore follows that if N is composite, it has at least one factor greater than p. Since N is either a prime greater than p or contains a prime factor greater than p, a prime larger than the largest in the finite sequence can always be found, so there are an infinite number of primes. Hardy (1967) remarks that this proof is "as fresh and significant as when it was discovered" so that "two thousand years have not written a wrinkle" on it.

Exercice

1. **Démonstration de cours** : démontrer qu'il existe une infinité de nombres premiers.

2. Soit p un nombre premier strictement plus grand que 2. Démontrer que p est congru à 1 ou à –1 modulo 4. Donner deux exemples de chacun de ces cas.

Le but de ce qui suit est de répondre à la question suivante :

« Les nombres premiers p congrus à –1 modulo 4 sont-ils en nombre fini ? »

Supposons que ce soit le cas : soit n le nombre des nombres premiers congrus à –1 modulo 4, notons $A = p_1 p_2 \ldots p_n$ le produit de ces nombres et $B = 4A - 1$.

3. Montrer que B est congru à –1 modulo 4.

4. Soit q un diviseur premier de B. Montrer que q est distinct de chacun des nombres $p_1, p_2, \ldots, p_n$ précédents.

Montrer que parmi les diviseurs premiers de B, l'un au moins est congru à –1 modulo 4.

5. Quelle réponse apporter à la question posée ?

1-g : Décomposition en produits de facteurs premiers

La démonstration n'est pas très drôle. Le lecteur peut consulter

http://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_fondamental_de_l%27arithm%C3%A9tique

Exercice 1

1. On considère le nombre $n = 200 = 2^3 5^2$.

a. Combien n a-t-il de diviseurs ? En utilisant un arbre, calculez les tous et faites leur somme s.

b. Vérifiez que $s = (1 + 2 + 2^2 + 2^3)(1 + 5 + 5^2)$.

2. On considère maintenant le nombre $N = a^\alpha b^\beta$ où a et b sont deux nombre premiers.

a. Quel est le nombre de diviseurs de N ?

b. Soit S la somme des diviseurs de N. Montrez que $N = (1 + a + a^2 + \ldots + a^\alpha)(1 + b + b^2 + \ldots + b^\beta)$.

c. Déduisez en une expression « simple » de S. Montrez alors que pour α et β suffisamment grands on a $\frac{S}{N} \approx \frac{a}{a-1} . \frac{b}{b-1}$.

Application numérique : $N = 5^{100} 7^{200}$; trouver une valeur approchée de S.

Exercice 2

Pour tout entier $n \geq 1$ on pose $u_n = 1! + 2! + \ldots + n!$

On donne la décomposition en facteurs premiers des dix premiers termes de la suite (u_n).

$u_1 = 1$ $\qquad$ $u_6 = 3^2 \times 97$

$u_2 = 3$ $\qquad$ $u_7 = 3^4 \times 73$

$u_3 = 3^2$ $\qquad$ $u_8 = 3^2 \times 11 \times 467$

$u_4 = 3 \times 11$ $\qquad$ $u_9 = 3^2 \times 131 \times 347$

$u_5 = 3^2 \times 17$ $\qquad$ $u_{10} = 3^2 \times 11 \times 40787$

1. Montrer que u_n n'est jamais divisible par 2, par 5 ni par 7.

2. Peut-on affirmer que u_n est divisible par 11 à partir d'un certain rang ?

3. Peut-on affirmer que, à partir d'un certain rang, u_n est divisible par 3^2 mais pas par 3^3 ?

1-h : Petit théorème de Fermat

Voici une démonstration due à Leibniz (il n'est pas sûr que ce dernier connaissait celle de Fermat).

Exercice 1

On considère l'expression $Z_n = (u_0 + u_1 + u_2 + \ldots + u_n)^p - (u_0^p + u_1^p + u_2^p + \ldots + u_n^p)$ où u_0, u_1, u_2, … , u_n sont des entiers quelconques (dont la somme n'est pas divisible par p) et p un nombre premier. Montrer par récurrence sur n que Z_n est divisible par p. Retrouver ainsi la démonstration du théorème de Fermat.

Exercice 2

1. Le nombre $2^{11} - 1$ est-il premier ?

2. p et q étant deux entiers naturels non nuls, quel est le reste de la division par $2^p - 1$ du nombre $2^{pq} = (2^p)^q$? En déduire que $2^{pq} - 1$ est divisible par $(2^p - 1)$ et $(2^q - 1)$.

3. Démontrer que, si $2^n - 1$ est premier, alors n est premier. Réciproque ?