EXERCICES D'ARITHMETIQUE

EXERCICE1 Guesmi.B

Nombres de Mersenne:

a: Montrez que pour tout n entier naturel > 2 , si $2^n - 1$ est premier alors n est premier

b: Montrez que $2^{11} - 1$ n'est pas premier

EXERCICE2

---

2. Le petit Théorème de FERMAT: (4è annee)

Soit p un entier naturel premier et n un entier strictement compris entre 0 et p.

a: Montrer que est divisible par p.

b : Montrez que, pour tout entier naturel a, $(a + 1)^p - a^p - 1$ est divisible par p.

c : Montrez que, pour tout b entier naturel, si $(b^p - b)$ est divisible par p alors $(b +1)^p -(b +1)$ l'est aussi.

d : Déduisez-en le petit théorème de Fermat:"**Pour tout entier p premier et tout a entier ,**

$a^p \equiv a$ [p] "

e: Montrez que p est premier si et seulement si pour tout r $\in\{1 ; 2 ; ... ; p - 1\}$, on a $r^{p-1} \equiv 1$ [p]

EXERCICE3(4è annee)

3. Soit p un entier naturel premier. On note Ep l'ensemble {1 ; 2 ; .... ; p-1}.

a : Montrez que tout élément de Ep est premier avec p.

b : Montrez que pour tout a de Ep , il existe b unique dans Ep tel que $ab \equiv 1$ [p].

c : Déterminez les a éléments de Ep tels que $a^2 \equiv 1$ [p].

d : Montrez que $1x2x3...x(p-1) \equiv(p -1)$ [p]

e : Déduisez-en que pour tout p entier naturel premier, (p -1)! + 1 est divisible par p

EXERCICE4

Montrez que si un entier naturel a exactement trois diviseurs dans N alors cet entier est le carré d'un nombre premier.

EXERCICE5

. Montrez que pour tout couple d'entier relatifs (x , y) , si $x^2 + y^2$ est divisible par 7 alors x et y sont aussi divisibles par 7

EXERCICE6

. p est un nombre premier > 2.

On suppose qu'il existe a et b dans N tels que $p = a^2 + b^2$.

a: Déterminez les valeurs p < 100 possibles.

b: Montrez que pour tout x dans N, x^2 est congru à 0 ou 1 modulo 4.

c: Montrez alors que p est congru à 1 modulo 4.
d: Peut-écrire 2003 comme somme de deux carrés dans N?

EXERCICE7(4è annee)

p est un nombre premier. On note E l'ensemble {0 ; 1 ; 2 ; ... ; p - 1}et E* l'ensemble E privé de 0.
a: Montrez que pour tout a E*, il existe b E* unique tel que $ab \equiv 1$ [p].
b: Montrez que pour tout (a , b) dans E , on a : $ab \equiv 0$ [p] $\Rightarrow$(a = 0 ou b = 0).
c: Montrez que pour tout X appartenant à E*, il existe au plus deux éléments dans E* vérifiant $x^2 \equiv X$ [p]
d: Déterminez les x E* tels que $x \equiv 1$ [p].
On pose p = 13.
e: Quelles sont les valeurs possibles X appartenant à E telles qu'il existe x dans E tel que $x^2 \equiv X$ [p]?
f: Déterminez l'ensemble de x dans Z vérifiant l'équation $x^2 + 2x + 3 \equiv 0$ [p].
g: Déterminez l'ensemble des x dans Z tels que $x^2 + 5x - 6$ soit divisible par 13

EXERCICE8

En reprenant l'exercice 7: , résolvez les équations suivantes:
a: $x^2 + 5x \equiv 0$ [5]
b: $x^2 - 5x + 2 \equiv 0$ [7]
c: $2x^2 + 4x + 1 \equiv 0$ [7]
d: $(x^2 - 1)^2 \equiv 9$ [11

EXERCICE9

Deux nombres premiers n et m sont dits "jumeaux" si n + 2 = m.
Par exemple , les couples (11 , 13) , (17 , 19) , (41 , 43) sont des couples de nombres premiers jumeaux.
a: Montrez que si (n , n + 2) est un couple de nombres premiers jumeaux alors n doit être congru à 2 modulo 3, autrement dit, on doit avoir , $n \equiv 2$ [3].
b: Montrez que si (n , n +2) est un couple de nombres premiers jumeaux alors n+ 4 ne peut pas être premier.
c: Montrez que (n , n +2) est un couple de nombres premiers jumeaux si et seulement si $n^2 + 2n$ a exactement 4 diviseurs dans N

EXERCICE10

Montrez que, pour tout b entier ≥ 3 , le nombre $x = 1 + b + 2b^2 + b^3 + b^4$ n'est pas un nombre premier

CORRECTION

EXERCICE1

a: Faisons un raisonnemnt par l'absurde. Supposons que n ne soit pas premier. On a donc n = ab avec a et b entiers > 1.
Rappelons l'identidé : $X^k - 1 = (X-1)(X^{k-1} + X^{k-2} + ... + X + 1)$.
On peut alors écrire:
$2^{ab} - 1 = (2^a)^b - 1 = (2^a -1)[(2^a)^{b-1} + (2^a)^{b-2} + ... + 1]$, produit de deux entiers > 1.
D'où 2^{ab}-1 n'est pas premier d'où la conclusion

b: $2^{11} - 1 = 2047 = 23 \times 89$ donc 2^{11}-1 n'est pas premier

EXERCICE2

a: Si p est premier et si n est entier avec 0 < n < p , alors:

On a donc la relation :

b: Il suffit alors , pour voir que $(a + 1)^p - a^p - 1$ est divisible par p, d'utiliser la formule du binôme de Newton, et de constater qu'en développant $(a + 1)^p - a^p - 1$, il ne reste que des termes divisibles par p, d'après la question précédente.

c: Même principe que la question précédente mais en faisant une récurrence sur b.

d: Conséquence directe des questions c: et b:

e: p est premier si et seulement si p est premier avec tout entier r appartenant à {1;2;...;p-1}.
Si p est premier alors pour tout r dans {1;2;...;p-1}, on a $(r^p - r)$ divisible par p.
Or, $(r^p - r) = r(r^{p-1} - 1)$.
Comme p et r sont premiers entre eux , on a alors $(r^{p-1} - 1)$ divisible par p, ou encore, $r^{p-1} \equiv 1$ [p

EXERCICE3

a: Evident car tout si a et p , avec a dans Ep ont un diviseur d > 1commun alors d est inférieur à a donc stirctement inférieur à p et comme p est premier, la seule valeur possible pour d est 1.

b: Si a est dans Ep, comme a et p sont premiers entre eux, on sait d'après le théorème de Bachet-Bezout, qu'il existe deux entiers naturels u et v tels que au+pv=1.

Soit u = Qp + b la division euclidienne de u par p. On a b dans {1;2;...;p-1}.

Effectivement, si b = 0 alors au + pv est divisble par p , ce qui contredit l'égalité au+pv=1.

Alors au + pv = a(Qp+b) + pv = ab + (aQ+v)p = 1

On a donc ab $\equiv$1 [p]. L'existence de b est donc assurée.

Pour l'unicité, supposons qu'il existe un autre entier c dans Ep tel que ac $\equiv$1 [p]

Alors a(b-c) est divisble par p. Comme a est premier avec p, on a donc (b-c) divisible par p.

Or, (b-c) est compris entre -(p-1) et (p-1) donc il ne peut pas être divisible par p. D'où l'unicité de b.

c: a^2 $\equiv$1 [p] si et seulement si (a-1)(a+1) est divisible par p.

a = 1 et a = (p-1) sont deux solutions évidentes.

Si a est dans {2;3;...;p-2} alors (a-1) et (a+1) sont dans {1;2;...;p-1}, donc premiers avec p.

Dans ce cas (a-1)(a+1) ne pas être divisible par p (car p premier).

Les seules solutions sont donc 1 et (p-1).

d: Pour p = 2,le résultat est évident car dans ce cas (p-1)! = 1! = 1 = (p-1) [p]. Pour p > 2 et premier:

Pour k compris strictement entre 1 et (p-1), il existe un k' unique distinct de k compris strictement entre 1 et (p-1) tel que kk' $\equiv$1 [p].

Dans le produit 1*2*3*...*(p-2)*(p-1), on regroupe alors les facteurs compris entre 2 et (p-2) deux par deux tels que le produit de ces facteurs soit identique à 1.

On a donc 1*(aa')*(bb')*(cc')*.....(dd')*(p-1) = 1*2*3*...*(p-1).

ce qui s'écrit 1*(p-1) $\equiv$1*2*3*...*(p-1) [p] d'où 1*2*3*...*(p-1) $\equiv$(p-1) [p].

e: Comme (p-1) $\equiv$-1 [p], on en déduit que 1*2*3*...*(p-1) +1 $\equiv$0 [p]

ou encore (p-1)! + 1 $\equiv$0 [p], c'est à dire (p-1)! + 1 est divisible par p

EXERCICE4

Soit n un entier naurel ayant exactement 3 diviseurs dans .

Comme 1 et n divise n, il existe alors un unique entier naturel non nul k $\in$ distincts de 1 et n divisant n.

Il existe donc un entier naturel q tel tel n = kq.

q est donc égal soit à 1 , soit à n, soit à k.

- Si q = 1 alors comme n = kq , on a alors k = n ..... c'est NON car k est distinct de n.

- Si q = n alors comme n = kq , on a alors k = 1 .... c'est NON car k est distinct de 1.

- Il reste alors q = k .... on a alors $n = k \times k = k^2$.

Donc, n est le carré d'un entier k non nul! et et on a k < n.

Mais si k n'est pas premier, alors k admet au moins un diviseur a distinct de 1 et de k.

a est alors < k ..... donc a est distinct de n.

Donc, comme a divise k et que k divise n, a divise n.

n admet alors au moins 4 diviseurs distincts à savoir 1, a , k et n.

Incompatible avec le fait que n a exactement 3 diviseurs...

Donc, k n'a aucun diviseur autre que 1 et k ... k est donc premier!

Donc, n est bien le carré d'un nombre premier.

Autre démonstration ... avec la décomposition en facteurs premiers!

Supposons que n admettent au moins deux diviseurs premiers distincts p et m.

On peut alors écrire que $n = p^a \times m^b \times K$ avec K premiers avec p et m.

Mais alors 1 , p , m et pm divise n ... donc n a au moins 4 diviseurs premiers .. Contradiction avec le fait que n a exactement 3 diviseurs!

Donc, n est diisible par un seul nombre premierp.

On a donc: $n = p^a$ avec a $\in$.

Mais le nombre de diviseurs de p^a est (a+1).

On a donc a+1 = 3 .... d'où .. a= 2 .... d'où $n = p^2$.

n est bien le carré d'un nombre premier

EXERCICE5

Soit x et y entiers tels $x^2 + y^2$ soit divisible par 7...ou encore ..$x^2 + y^2 \equiv 0$ [7]

Les carrés modulo 7 sont:

- $0^2 \equiv 0$ [7]
- $1^2 \equiv 1$ [7]
- $2^2 \equiv 4$ [7]
- $3^2 \equiv 2$ [7]
- $4^2 \equiv 2$ [7]
- $5^2 \equiv 4$ [7]
- $6^2 \equiv 1$ [7]

D'où, pour tout couple d'entier (x ; y) , on a $x^2 + y^2 \equiv 0$ [7] $\Longleftrightarrow$ x et y $\equiv 0$ [7]

D'où ... la réponse

EXERCICE6

a) Faites la liste .....

b)Pour tout x dans Z, on a x congru à 0 ou 1 ou 2 ou 3 modulo 4.
Donc, x^2 est congru à 0^2 ou 1^2 ou 2^2 ou 3^2 modulo 4.
D'où x^2 est congru à 0 ou 1 modulo 4.

c) Comme p est un nombre premier > 2, p est impair donc congru à 1 ou 3 modulo 4.
$p = a^2 + b^2$. Or, a^2 et $b^2 \equiv 0$ ou 1 modulo 4.
Donc, modulo 4, les valeurs possibles de $a^2 + b^2$ sont 0 ou 1 ou 2.
Comme p est congru à 1 ou 3 modulo 4, on a alors p congru à 1 modulo4.

d) 2003 est premier (faites-vous la vérification!)
De plus, 2003 = 3 modulo 4.

Donc, d'après la question précédente, 2003 ne peut s'écrire sous la forme a^2+b^2 avec a et b entiers

EXERCICE7

p est un nombre premier. On note E l'ensemble {0 ; 1 ; 2 ; ... ; p - 1}et E* l'ensemble E privé de 0.

a: Montrez que pour tout a E*, il existe b E* unique tel que ab $\equiv$ 1 [p].

Si a $\in$E* alors a et p sont premiers entre eux.

Donc, d'après le Théorème de Bezout, il existe u et v dans tels que **au + pv = 1**.

Donc, il existe u $\in$ tel que **au $\equiv$1 [p]**.

Posons alors b = reste dans la division euclidienne de u par p. On a alors **b $\equiv$u [p]**.

Donc, **ab $\equiv$1 [p]** .. il existe donc bien b $\in$E* tel que ab $\equiv$1 [p].

Supposons alors qu'il existe deux entiers b et c $\in$E* tels que ab $\equiv$1[p] et ac $\equiv$1 [p]. On a par exemple, b $\geq$c.

On a alors a(b-c) $\equiv$0 [p]. Donc a(b-c) est divisible par p.

Mais, a et p sont premiers entre eux, donc, d'après le Théorème de Gauss, p divise (b-c).

Mais , b et c sont inférieurs à (p-1). Donc, (b-c) $\leq$(p-1).

Donc, (b-c) est divisible par p mais (b-c) $\leq$(p-1).....Donc, (b-c)=0 ..d'où b = c.

Conclusion:

Il existe bien b $\in$E* unique tel que ab $\equiv$1 [p]

b: Montrez que pour tout (a , b) dans E , on a : ab $\equiv$0 [p] $\Rightarrow$(a = 0 ou b = 0).

Supposons que a et b soient non nuls.

a et b $\in$E*, donc a et b sont premiers avec p. Mais ab $\equiv$0 [p], c'est à dire, ab est divisible par p.

p divise ab donc p divise a ou b. Impossible ...a et b premiers avec p ...

Donc, a =0 ou b = 0.

c: Montrez que pour tout X appartenant à E*, il existe au plus deux éléments dans E* vérifiant x^2 $\equiv$X [p]

Supposons qu'il existe trois éléments distincts a,b et c de E* vérifiant l'équation x^2 $\equiv$X [p].

On a alors a^2 $\equiv$$b^2$ [p] ...donc (a-b)(a+b) $\equiv$0 [p].

Donc, comme (a-b) est premiers avec p, on a: a+b $\equiv$[p].

De même, a+c $\equiv$0 [p].

On a alors $a \equiv -b$ [p] et $a \equiv -c$ [p] ...d'où .. $b \equiv c$ [p].

Mais b et c $\in$ E*...donc b = c.

Donc, il existe bien au plus deux solutions dans E* pour l'équation $x^2 \equiv X$ [p].

d: Déterminez les x E* tels que $x^2 \equiv 1$ [p].
On sait que $1^2 = 1$ et $(-1)^2 = 1$.

Donc, 1 et -1 sont des solutions de l'équation dans $x^2 \equiv 1$ [p].

Mais $-1 \equiv (p-1)$ [p].

Donc, 1 et (p-1) sont les seules solutions dans E* de l'équation $x^2 \equiv 1$ [p].

On pose p = 13.
e: Quelles sont les valeurs possibles X appartenant à E telles qu'il existe x dans E tel que $x^2 \equiv X$ [p]?
Il suffit de faire défiler les carrés modulo 13 de x, pour x variant dans E.

$0^2 = 0 \equiv 0$ [13]
$1^2 = 1 \equiv 1$ [13]
$2^2 = 4 \equiv 4$ [13]
$3^2 = 9 \equiv 9$ [13]
$4^2 = 16 \equiv 3$ [13]
$5^2 = 25 \equiv 12$ [13]
$6^2 = 36 \equiv 10$ [13]
$7^2 = 49 \equiv 10$ [13]

On peut remarquer alors que pour x > 7 , (13-x) < 6 et $(13-x)^2 \equiv x^2$ [13].

Les carrés modulo 13 sont donc 0 , 1 , 4 , 9 , 3 , 12 , 10.

f: Déterminez l'ensemble de x dans Z vérifiant l'équation $x^2 + 2x + 3 \equiv 0$ [p].
On pense à la forme canonique!

$x^2 + 2x + 3 = (x+1)^2 + 2$.

$x^2 + 2x + 3 \equiv (x+1)^2 + 2$ [13] donc $x^2 + 2x + 3 \equiv 0$ [13] $\Longleftrightarrow (x+1)^2 \equiv -2$ [13].

Mais, $-2 \equiv 11$ [13]...on a donc $x^2 + 2x + 3 \equiv 0$ [13] $\Longleftrightarrow (x+1)^2 \equiv 11$ [13].

Mais, 11 n'est pas un carré modulo 13 ... donc il n'existe pas de x dans tel que $x^2+2x+3 \equiv 0$ [13].

g: Déterminez l'ensemble des x dans Z tels que $x^2 + 5x - 6$ soit divisible par 13.
On remarque que $5 \equiv 2 \times 9$ [13].

On a donc : $x^2 + 5x - 6 \equiv 0$ [13] $\Longleftrightarrow x^2 + 2 \times 9x - 6 \equiv 0$ [13].

Mais, $x^2 + 18x - 6 = (x + 9)^2 - 9^2 - 6$.

Mais $9^2 \equiv 3$ [13], donc $x^2 + 18x - 9 \equiv 0$ [13] $\Longleftrightarrow (x+9)^2 - 9 \equiv 0$ [13]

D'où : $x^2 + 18x - 6 \equiv 0$ [13] mod sii mod:: 0 [13].

Donc, $x^2 + 5x - 6$ est divisible par 13 $\Longleftrightarrow$ (x-7)(x-1) est divisible par 13.

Mais 13 est premier, donc (x-1)(x-12) divisible par 13 $\Longleftrightarrow$ (x-7) OU (x-1) divisible par 13.

Donc $\Longleftrightarrow$ il existe k $\in$ tel que x = 13k + 7 OU x = 13k + 1.

Les solutions de l'équation dans sont donc les entiers congrus à 7 ou 1 modulo 13