Exercices d'arithmétiques

18 janvier 2014

Exercice 1. *1. Montrer que si n est somme des carrés de deux entiers consécutifs alors $2n-1$ est le carré d'un entier.*

2. Montrer que si $2n-1$ est le carré d'un entier alors n est somme des carrés de deux entiers consécutifs.

Exercice 2. *Montrer qu'il existe une infinité d'entiers $a \in \mathbb{N}$ tels que $n^4 + a$ n'est premier pour aucun entier $n \in \mathbb{N}$.*

Exercice 3. *Déterminer $(2^m - 1) \wedge (2^n - 1)$.*

Exercice 4. *Déterminer tous les couples d'entiers a, b tels que $a^b = b^a$.*

Exercice 5. *Trouver tous les entiers a et b tels que $7^a - 3 \times 2^b = 1$.*

Exercice 6 (OIM 2002-4)**.** *Soit n un entier strictement plus grand que 1. On note $d_1, d_2, \cdots, d_k$ les diviseurs positifs de n avec*

$$1 = d_1 < d_2 < \cdots < d_k = n.$$

On pose $D = d_1 d_2 + d_2 d_3 + \cdots + d_{k-1} d_k$.

Montrer que $D < n^2$.

Trouver les n tels que D est un diviseur de n^2.

Exercice 7. *Existe-t-il des entiers $n \geqslant 1$ tels que 9 divise $7^n + n^3$?*

Exercice 8. *Déterminer le nombre des dizaines de milliers de $A = 5^{5^{5^{5^5}}}$.*

Exercice 9 (OIM 99-4)**.** *Déterminer les couples d'entiers strictement positifs (n, p) tels que*

- *p est un nombre premier,*
- *$n \leqslant 2p$,*
- *$(p-1)^n + 1$ est divisible par n^{p-1}.*

Exercice 10 (OIM 1990-4)**.** *Déterminer les entiers $n \in \mathbb{N}$ tels que $n^2 \mid 2^n + 1$.*

Solutions des exercices d'arithmétiques

18 janvier 2014

Exercice 1. 1. *Montrer que si n est somme des carrés de deux entiers consécutifs alors $2n-1$ est le carré d'un entier.*

2. *Montrer que si $2n-1$ est le carré d'un entier alors n est somme des carrés de deux entiers consécutifs.*

Solution 1. 1. Par hypothèse, il existe un entier a tel que $n = a^2 + (a+1)^2$. On développe ce qui donne :

$$n = 2a^2 + 2a + 1.$$

Un calcul donne maintenant que

$$2n - 1 = 4a^2 + 4a + 1 = (2a)^2 + 2 \times (2a) \times 1 + 1^2.$$

On reconnaît une identité remarquable :

$$2n - 1 = (2a+1)^2$$

ce qui prouve bien que $2n-1$ est le carré d'un entier.

2. Par hypothèse, il existe un entier b tel que $2n-1 = b^2$. De plus, comme $2n-1$ est impair, on remarque que b est aussi forcément impair (le carré d'un entier pair est pair et le carré d'un entier impair est impair). Ainsi, il existe un entier a tel que $b = 2a+1$. On a donc

$$2n - 1 = (2a+1)^2 = 4a^2 + 4a + 1.$$

Ainsi un calcul donne que

$$n = 2a^2 + 2a + 1 = a^2 + (a^2 + 2a + 1) = a^2 + (a+1)^2.$$

Comme a est entier, on a bien montré que n est somme de deux entiers consécutifs.

Exercice 2. *Montrer qu'il existe une infinité d'entiers $a \in \mathbb{N}$ tels que $n^4 + a$ n'est premier pour aucun entier $n \in \mathbb{N}$.*

Solution 2. Il faut bien choisir la forme de a. Pour $a = 4k^4$, on peut utiliser les identités remarquables comme suit :

$$n^4 + 4k^4 = (n^2 + 2k^2)^2 - 4n^2k^2 = (n^2 + 2k^2 - 2nk)(n^2 + 2k^2 + 2nk).$$

De plus $n^2 + 2k^2 - 2nk = (n-k)^2 + k^2$, donc $n^4 + 4k^4$ n'est jamais premier dès que $k \geqslant 2$ (pour $k = 1$ on a $1 + 4 = 5$...).

Exercice 3. *Déterminer* $2^m - 1 \wedge 2^n - 1$.

Solution 3. Écrivons la division euclidienne de n par m : $n = qm + r$. Maintenant on cherche à faire celle de $2^n - 1$ par $2^m - 1$:

$$2^n - 1 = (2^{mq} - 1)2^r + 2^r - 1 = (2^m - 1)(1 + 2^m + 2^{2m} + \cdots + 2^{(q-1)m}) + 2^r - 1.$$

De plus, $2^r - 1 < 2^m - 1$. Ainsi, l'algorithme d'Euclide associé à $2^n - 1$ et $2^m - 1$ peut être fait parallèlement à celui de n et m. Si $d = n \wedge m$, on aura

$$2^m - 1 \wedge 2^n - 1 = 2^d - 1.$$

Exercice 4. *Déterminer tous les couples d'entiers a, b tels que $a^b = b^a$.*

Solution 4. On commence, comme d'habitude, par introduire $d = a \wedge b$ et écrire $a = da'$ et $b = db'$ où $a' \wedge b' = 1$.

On constate d'abord que $a = b$ est toujours solution.

On cherche les autres solutions. Sans perte de généralité (quitte à inverser les rôles de a et b), on va supposer que $a < b$. Ainsi, l'équation se réécrit

$$d^{b-a}a'^b = b'^a.$$

On voit tout de suite que $a' = 1$ car $a' \mid b'^a$ alors que $a' \wedge b'^a = 1$. Et donc $d = a$ et $b' \geqslant 2$:

$$d^{d(b'-1)} = b'^d.$$

On prend les racines d-ièmes :

$$d^{b'-1} = b',$$

et on a encore quelques cas à traiter. Si $d = 1$, alors $b' = 1$ ce qui n'est pas possible, on a exclu ce cas.

Si $d = 2$, on voit que pour $b' = 2$ on a une solution qui correspond à $a = 2, b = 4$. Ensuite, on montre (par récurrence ou par une étude de fonction) que pour $b' > 2$, alors $2^{b'-1} > b'$.

Enfin, si $d \geqslant 3$, la situation est encore plus dramatique et on montre que

$$d^{b'-1} \geqslant 3^{b'-1} > b'.$$

Ainsi, les seuls solutions sont les couples (a, a), $(2, 4)$ et $(4, 2)$.

Exercice 5. *Trouver tous les entiers a et b tels que $7^a - 3 \times 2^b = 1$.*

Solution 5. On voit que $a = 0$ ou $b = 0$ sont impossibles. On réécrit l'équation comme suit :

$$7^a - 1 = 6 \times \sum_{i=0}^{a-1} 7^i = 6 \times 2^{b-1}.$$

Si $a = 1$, alors $b = 1$ est l'unique solution. Si $a = 2$ alors $b = 4$ est l'unique solution.

Supposons maintenant que $a > 2$ ce qui implique que $b > 4$. Comme la somme de gauche est paire, mais constituée d'élément impaires, il doit y avoir un nombre pair de terme, a est donc pair. On regroupe termes pairs et impairs pour obtenir

$$(7+1) \sum_{i=0}^{a/2-1} 7^{2i} = 8 \times 2^{b-4}.$$

On simplifie, et on se rappelle que comme $b > 4$, la somme de gauche est paire mais encore constituée de termes impairs. Il y a donc un nombre pair de termes ($a/2$ est pair) et on peu recommencer la procédure :

$$(7^2+1) \sum_{i=0}^{a/4-1} 7^{4i} = 2^{b-4},$$

on aboutit à une contradiction car une puissance de 2 n'est pas divisible pas 50.

Les seules solutions sont donc $(1, 1)$ et $(2, 4)$.

Exercice 6 (OIM 2002-4)**.** *Soit n un entier strictement plus grand que 1. On note $d_1, d_2, \cdots, d_k$ les diviseurs positifs de n avec*

$$1 = d_1 < d_2 < \cdots < d_k = n.$$

On pose $D = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$.

Montrer que $D < n^2$.

Trouver les n tels que D est un diviseur de n^2.

Solution 6. Il est clair que pour tout m, $d_{k-m} \leqslant n/(m+1)$. Ainsi, il vient que

$$\begin{aligned} D \leqslant n^2 \Big(\frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \cdots + \frac{1}{(k-1) \times k} \Big) \\ = n^2 \Big(\frac{1}{1} - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \cdots + \frac{1}{k-1} - \frac{1}{k} \Big) \\ = n^2 \Big(1 - \frac{1}{k} \Big) < n^2. \end{aligned}$$

Pour la seconde partie de la question, on commence par remarquer que si n est premier, alors $D = d_1 d_2 = n \mid n^2$.

Si n est composé, soit $p = d_2$ le plus petit diviseur premier de n. Alors

$$n^2 > D > d_{k-1} d_k = n \times \frac{n}{p} = \frac{n^2}{p}.$$

Mais c'est alors impossible que $D \mid n^2$ car n^2/p est le plus grand diviseur strict de n^2.

Exercice 7. *Existe-t-il des entiers $n \geqslant 1$ tels que 9 divise $7^n + n^3$?*

Solution 7. La réponse est non, voyons pourquoi. Soit n comme demandé. On a que n^3 est congru à 0, 1 ou -1 modulo 9 (c'est toujours vrai). Mais ici, n^3 ne peut pas être divisible par 9, donc on obtient que $n^6 \equiv 1[9]$. En particulier, $7^{2n} \equiv 1[n]$. Donc $2n$ est un multiple de l'ordre de modulo 9. Cet ordre étant 3, n est un multiple de 3. C'est problématique vu que n^3 n'est pas divisible pas 9 !

Exercice 8. *Déterminer le nombre des dizaines de milliers de $A = 5^{5^{5^{5^5}}}$.*

Solution 8. On va déterminer le reste de la division euclidienne de A par $10000 = 2^5 \times 5^5$. On commence par diviser par 2^5. Comme $\varphi(2^5) = 16$, il suffit de déterminer le reste de la division euclidienne de $5^{5^{5^5}}$ par 16 et enfin, comme $\varphi(16) = 8$, il faut déterminer le reste de 5^{5^5} par 8. Et enfin 5^5 par 4 soit 1.

Donc on remonte $5^{5^5} \equiv 5[8]$, $5^{5^{5^5}} \equiv 5^5 \equiv 13[16]$. Et enfin, $A \equiv 5^{13} \equiv 5^5[2^5]$.

Ouf, il vient que l'on n'est pas obligé de refaire tout le travail pour 5^5, on a immédiatement $A \equiv 5^5 = 3125[10000]$. Ainsi, le chiffre de dizaines de milliers de A est 0.

Exercice 9 (OIM 99-4)**.** *Déterminer les couples d'entiers strictement positifs (n, p) tels que*

- *p est un nombre premier,*
- *$n \leqslant 2p$,*
- *$(p-1)^n + 1$ est divisible par n^{p-1}.*

Solution 9. On trouve d'abord des solutions évidentes : $(1, p)$ est toujours solution.

Si $p = 2$, et $n > 1$ alors seul $n = 2$ fonctionne et $(2, 2)$ est solution.

On suppose désormais que $p \geqslant 3$. Ainsi, n est nécessairement impair. Comme il est toujours plus simple de travailler avec des nombres premiers, soit q premier tel que $q \mid n$. Alors, les hypothèses impliquent $(p-1)^n \equiv -1[q]$, et plus généralement, $(p-1)^{an} \equiv (-1)^a[q]$. Fermat nous apprend aussi que $(p-1)^{b(q-1)} \equiv 1[q]$ car $p-1$ n'est pas divisible par q. On résume :

$$(p-1)^{an+b(q-1)} \equiv (-1)^a[q].$$

On se demande maintenant pour quelles valeurs de a et b on peut obtenir quelque chose d'intéressant, et on pense à Bezout. Mais il faut pour l'utiliser que $q-1 \wedge n = 1$. Pour ce faire, on suppose que q est le plus petit diviseur premier de n (qui est impair) et on prend a et b donnés par Bezout, de sorte que $an+b(q-1) = 1$. On voit immédiatement que a doit être impair, et donc

$$p-1 \equiv -1[q]$$

soit $q \mid p$! Comme $n < 2p$ on a même que $n = p$, par minimalité de q.

On est prêt du but. En développant

$$(p-1)^p + 1 = \sum_{i=1}^{p} (-1)^{p-k} p^k \binom{p}{k} = p^2 + A,$$

on observe que A est divisible par p^3, donc $(p-1)^p+1$ n'est pas divisible par p^3. Ainsi, on obtient que $p \leqslant 3$, soit $p = 3$ et $(3,3)$ est bien une solution du problème, la dernière.

Exercice 10 (OIM 1990-4). *Déterminer les entiers $n \in \mathbb{N}$ tels que $n^2 \mid 2^n+1$.*

Solution 10. Les solutions évidentes sont 1 et 3. Supposons dorénavant que $n > 1$. Au hasard, considérons p le plus petit entier qui divise n. Il est clair que n doit être impair, et donc que p aussi. L'hypothèse implique que $2^n \equiv -1[p]$ et donc que $2^{2n} \equiv 1[p]$. Ainsi, l'ordre de 2 modulo p divise $2n$. Mais il divise également $p-1$ (petit théorème de Fermat) et par définition de p, $(p-1) \wedge n = 1$. Ainsi on obtient que cet ordre vaut 1 ou 2. Dans le premier cas, on trouve $2 \equiv 1[p]$ ce qui est impossible, la seconde possibilité, implique que $p = 3$. On écrit donc $n = 3^l \times k$ et on va déterminer les valeurs possibles de l. Pour cela, on factorise

$$2^{3^l k} + 1 = (2^{3^{l-1}k} + 1)(2^{2\times 3^{l-1}k} - 2^{3^{l-1}k} + 1).$$

On voit que cette formule (en particulier le terme de gauche) ce prête particulièrement bien à une récurrence. On évalue le terme de droite modulo 9. 2 est d'ordre 6 modulo 9 et ses premières puissances sont $2, 4, -1, -2, -4, 1$. En se rappelant que k est impair, on obtient immédiatement que

$$2^{2\times 3^{l-1}k} - 2^{3^{l-1}k} + 1 \equiv 3[9].$$

Enfin, 2^k+1 est aussi divisible par 3, mais pas par 9, du fait que k est impair, mais pas divisible par 3. En conclusion, la valuation de 3 dans $2^{3^l k}+1$ est exactement $l+1$. Mais par hypothèse, $3^{2l} \mid 2^n+1$, ainsi, la seule possibilité est que $k=1$.

Maintenant qu'on a réglé son compte à 3, on passe au diviseur premier suivant. On suppose $l \geqslant 2$, sinon on a la solutions $n=3$. Soit encore p le plus petit diviseur de l. Ainsi, $p \geqslant 5$, et on recommence comme tout à l'heure. De $2^{6l} \equiv 1[p]$ on déduit que l'ordre de 2 modulo p divise $6l$ mais aussi $p-1$ et donc par définition de p, il doit diviser 6. Il vaut dont 1, 2, 3, ou 6. Et on a que 2, 4, 8 ou 64 est congru à 1 modulo p. De tous ces cas, comme p n'est ni 2 ni 3, la seule possibilité est $p=7$. Mais 7 ne divise jamais 2^n+1, en effet les puissances successives de 2 modulo 7 sont $2, 4, 1$. Il n'y a donc pas d'autre solution.