Corrigé de l'envoi 1

1 Exercices groupe B

Exercice 1 Prouver qu'il n'existe qu'un nombre fini de nombres premiers s'écrivant sous la forme n^3+2n+3 avec $n \in \mathbb{N}$.

Solution de l'exercice 1: Remarquons que $n^3-n = n(n-1)(n+1)$ est un produit de trois entiers consécutifs. Puisque parmi trois entiers consécutifs il y a toujours un multiple de 3, on obtient que $n^3 - n$ est divisible par 3, c'est-à-dire $n^3 \equiv n \pmod 3$. (On peut le voir aussi en utilisant le petit théorème de Fermat.) On a donc $n^3 + 2n + 3 \equiv n + 2n + 3 \equiv 3n + 3 \equiv 0 \pmod 3$, donc $n^3 + 2n + 3$ est toujours divisible par 3. D'autre part, il ne peut être égal à 3 que pour un nombre fini de valeurs de n.

Exercice 2 Résoudre $x^4 - 6x^2 + 1 = 7 \times 2^y$ pour x et y entiers.

Solution de l'exercice 2: L'équation se réécrit $(x^2 - 3)^2 = 7 \times 2^y + 8$. Si $y \geq 3$, alors le côté droit s'écrit $8(7 \times 2^{y-3} + 1)$. Le côté gauche étant un carré, sa valuation 2-adique est paire. Ainsi, $7 \times 2^{y-3} + 1$ doit être pair, donc $y = 3$. Dans ce cas $x^2 - 3 = 8$ donc $x^2 = 11$, impossible. Donc $y \leq 2$. Si $y = 2$, on trouve $x = \pm 3$. Pour $y < 0$, ainsi que pour $y = 0$ ou $y = 1$ il n'y a pas de solution. Les seuls couples de solutions sont donc $(x, y) = (3, 2)$ et $(-3, 2)$.

Exercice 3 Trouver le plus petit entier positif qui ne s'écrit pas sous la forme $\frac{2^a-2^b}{2^c-2^d}$ pour $a, b, c, d \in \mathbb{N}$.

Solution de l'exercice 3: Soit E l'ensemble des entiers strictement positifs s'écrivant sous cette forme. Commençons par remarquer que

$$\frac{2^a - 2^b}{2^c - 2^d} = 2^{b-d}\frac{2^{a-b} - 1}{2^{c-d} - 1}.$$

Ainsi, si $x > 0$ s'écrit $x = \frac{2^a-2^b}{2^c-2^d}$, alors $b-d = v_2(x)$ et si on appelle y l'entier impair tel que $x = 2^{v_2(x)}y$, alors y s'écrit sous la forme $\frac{2^n-1}{2^m-1}$. En particulier, l'entier que nous cherchons est nécessairement impair. D'autre part, on peut tout de suite exclure les entiers de la forme $2^n - 1$, atteints avec $m = 1$.

Il est classique que si $2^m - 1$ divise $2^n - 1$, alors m divise n. Ainsi, en écrivant $n = md$, y est de la forme

$$y = \frac{2^{md} - 1}{2^m - 1} = 2^{(d-1)m} + 2^{(d-2)m} + \ldots + 2^m + 1.$$

Autrement dit, en notant $u = \underbrace{0 \ldots 0}_{m-1 \text{ zéros}} 1$, l'écriture en base 2 de y est de la forme $\overline{1u \ldots u}^2$, avec u apparaissant $d-1$ fois. Les entiers impairs appartenant à E sont exactement ceux ayant une telle écriture binaire pour m et d bien choisis. Les écritures binaires des premiers entiers impairs qui ne sont pas de la forme $2^n - 1$ sont

$$5 = \overline{101}^2,\ 9 = \overline{1001}^2, 11 = \overline{1011}^2.$$

D'après le critère ci-dessus, le plus petit entier cherché est 11.

Remarque : cet exercice peut aussi se faire en trouvant des manières d'écrire les entiers 1 à 10 sous cette forme, puis en montrant que 11 ne s'écrit pas sous cette forme : en effet, vu que 11 est impair, on peut supposer $b = d = 1$. Ensuite

$$(2^a - 1) = 11(2^c - 1)$$

se réécrit

$$10 = 2^c \times 11 - 2^a.$$

Puisque $10 = 2 \times 5$, nous avons $a = 1$ ou $c = 1$. Si $a = 1$, on trouve $2^c \times 11 = 12$, qui n'a pas de solution, et si $c = 1$, on trouve $2^a = 12$, qui n'a pas de solution non plus. Donc 11 est l'entier cherché.

2 Exercices communs

Exercice 4 Trouver tous les triplets de nombres premiers (p, q, r) tels que $(p+1)(q+2)(r+3) = 4pqr$.

Solution de l'exercice 4: Si $p = 2$ alors on a $3(q+2)(r+3) = 8qr$ ce qui implique $q = 3$ ou $r = 3$. On a alors la solution $(2, 3, 5)$.

Si $q = 2$ et $p, r > 2$ alors on a $(p+1)(r+3) = 2pr$. Puisque p et r sont impairs, le membre de gauche est divisible par 4, alors que le membre de droite est divisible par 2, mais pas par 4, contradiction. Donc p ou r vaut 2 mais aucune solution valide n'en découle.

Si $r = 2$ alors $5(p+1)(q+2) = 8pq$ et donc p ou q vaut 5. On obtient la solution $(7, 5, 2)$.

Sinon, $(p+1)$ est pair et $(r+3)$ est pair. Donc on se ramène à

$$\left(\frac{p+1}{2}\right)(q+2)\left(\frac{r+3}{2}\right) = pqr.$$

Nous avons donc écrit pqr comme un produit de trois facteurs strictement plus grands que 1. On en déduit que $(\frac{p+1}{2}, q+2, \frac{r+3}{2})$ est une permutation de (p, q, r).

Clairement, $p \neq \frac{p+1}{2}$ puisque $p > \frac{p+1}{2}$.

Si $p = \frac{r+3}{2}$, alors puisque $q \neq q+2$, nous avons nécessairement $q = \frac{p+1}{2} = \frac{r+5}{4}$. Alors $r = q+2 = \frac{r+13}{4}$, et donc r n'est pas entier.

Si $p = q+2$, alors il y a deux cas à considérer :

– $r = \frac{p+1}{2} = \frac{q+3}{2}$ et $q = \frac{r+3}{2} = \frac{q+9}{4}$. Donc $q = 3$ et on obtient la solution $(5, 3, 3)$.

– $r = \frac{r+3}{2}$ et $q = \frac{p+1}{2} = \frac{q+3}{2}$, ce qui donne $r = q = 3$. On obtient alors cette même solution $(5, 3, 3)$.

Finalement, les seules solutions sont $(2, 3, 5), (7, 6, 2)$ et $(5, 3, 3)$.

Exercice 5 Trouver tous les entiers strictement positifs n tels que $2^{n-1}n + 1$ soit un carré parfait.

Solution de l'exercice 5: On veut résoudre $2^{n-1}n + 1 = m^2$, c'est-à-dire $2^{n-1}n = (m-1)(m+1)$. Puisque $n = 1$ n'est pas solution, on a $n \geq 2$, et donc m est nécessairement impair, et $m-1$ et $m+1$ sont pairs (en particulier $n \geq 3$). On pose $k = \frac{m-1}{2}$. Il suffit alors de résoudre $2^{n-3}n = k(k+1)$. Parmi les entiers k et $k+1$ exactement un est pair, et donc ils sont de la forme $2^{n-3}d$ et $\frac{n}{d}$ avec d un diviseur de n. Or un diviseur de n ne peut pas être à distance 1 d'un entier supérieur à 2^{n-3} si n est trop grand. Plus précisément, on a $2^{n-3}d \geq 2^{n-3} \geq n+2$ si $n \geq 6$, donc on a nécessairement $n \leq 5$. Pour $n = 5$, on trouve $2^4 \times 5 + 1 = 9^2$, donc 5 est solution. On vérifie que $2, 3, 4$ ne sont pas solutions. Donc $n = 5$ est la seule solution.

Exercice 6 Soient $x > 1$ et y des entiers vérifiant $2x^2 - 1 = y^{15}$. Montrer que x est divisible par 5.

Solution de l'exercice 6: L'entier y est clairement impair et strictement plus grand que 1. On factorise l'équation sous la forme

$$x^2 = \left(\frac{y^5+1}{2}\right)(y^{10} - y^5 + 1).$$

Remarquons que

$$y^{10} - y^5 + 1 \equiv 3 \pmod{y^5+1},$$

et que donc $\text{pgcd}(y^5+1, y^{10}-y^5+1)$ est égal à 1 ou à 3. S'il valait 1, alors $y^{10}-y^5+1$ serait un carré. Or pour $y > 0$ nous avons

$$(y^5-1)^2 = y^{10} - 2y^5 + 1 < y^{10} - y^5 + 1 < y^{10} = (y^5)^2,$$

c'est-à-dire que $y^{10}-y^5+1$ est strictement compris entre deux carrés consécutifs, et ne peut pas être lui-même un carré. Donc $\text{pgcd}(y^5+1, y^{10}-y^5+1) = 3$, de sorte qu'il existe des entiers a et b tels que

$$y^5 + 1 = 6a^2 \quad \text{et} \quad y^{10} - y^5 + 1 = 3b^2.$$

On peut factoriser $(y+1)(y^4-y^3+y^2-y+1) = 6a^2$. Puisque $y^5 \equiv -1 \pmod 3$, on a nécessairement $y \equiv -1 \pmod 3$, donc $y+1$ est divisible par 6. De même que plus haut, on a

$$y^4 - y^3 + y^2 - y + 1 \equiv 5 \pmod{y+1},$$

et donc $\text{pgcd}(y+1, y^4-y^3+y^2-y+1)$ est égal à 1 ou à 5. S'il vaut 5, alors a est divisible par 5 et donc x aussi, et nous avons terminé. Supposons donc qu'il vaut 1. Alors $y^4-y^3+y^2-y+1$ est un carré. Dans ce cas, $4(y^4-y^3+y^2-y+1)$ est aussi un carré, ce qui est impossible, car pour $y > 1$, on a

$$(2y^2-y)^2 = 4y^4 - 4y^3 + y^2 < 4(y^4-y^3+y^2-y+1) < 4y^4 - 4y^3 + 5y^2 - 2y + 1 = (2y^2-y+1)^2.$$

3 Exercices groupe A

Exercice 7 Caractériser les entiers $n \geq 2$ tels que pour tout entier a on ait $a^{n+1} = a \pmod{n}$.

Solution de l'exercice 7: Voici les n vérifiant cette propriété : $2,\ 2\cdot 3,\ 2\cdot 3\cdot 7,\ 2\cdot 3\cdot 7\cdot 43$.

Pour prouver que c'est exhaustif on procède de la façon suivante : on commence par remarquer que n n'a pas de facteur carré. En effet, si p^2 divise n, alors $p^{n+1}-p$ est divisible par p^2, ce qui n'est pas possible. Ainsi, n est forcément un produit $p_1 \dots p_k$ de nombres premiers distincts. Par conséquent, par le lemme chinois la condition de l'énoncé est équivalente à $a^{n+1} \equiv a \pmod{p}$ pour tout entier a et tout $p \in \{p_1, \dots, p_k\}$. En choisissant a d'ordre $p-1$ modulo p, on obtient que cela est équivalent à ce que $p-1$ divise n pour tout $p \in \{p_1, \dots, p_k\}$.

En résumé : n est produit de premiers distincts $p_1, \dots, p_k$, et $p_i - 1$ divise n pour tout i. On en déduit que pour tout i, $p_i - 1$ est sans facteur carré et $p_i - 1 = q_1 \dots q_m$ où les q_j sont des nombres premiers pris parmi les p_r, $r \neq i$.

Quitte à re-numéroter les p_i, on peut supposer que $p_1 < p_2 < \dots < p_k$. D'après la condition ci-dessus, nous avons nécessairement $p_1 = 2$. Si $k = 1$, cela nous donne l'entier $n = 2$. Si $k > 1$, alors $p_2 - 1$ est nécessairement égal à 2, donc $p_2 = 3$. Si $k = 2$, cela nous donne la solution $n = 6$. Si $k > 2$ on continue en disant que $p_3 - 1$ ne peut être égal à 2 ou 3, donc il est égal à $p_1 p_2 = 6$, d'où $p_3 = 7$. Si $k = 3$, cela donne la solution $n = 2\cdot 3\cdot 7 = 42$. Si $k > 3$, on voit que de même la seule valeur possible pour p_4 est $2\times 3\times 7+1 = 43$. Pour $k = 4$, cela donne la solution $n = 2\cdot 3\cdot 7\cdot 43$. Enfin, supposons que $k > 4$. Alors $p_5 - 1$ doit être pair et strictement supérieur à 43, donc les seules valeurs possibles sont $2\cdot 43, 2\cdot 3\cdot 43, 2\cdot 7\cdot 43, 2\cdot 3\cdot 7\cdot 43$. On vérifie qu'aucune de ces possibilités ne fournit un p_5 premier. Ainsi on a nécessairement $k \leq 4$ et les solutions que nous avons trouvées sont les seules.

Exercice 8 Soit $k \geq 3$ un entier. On définit la suite $(a_n)_{n\geq k}$ par $a_k = 2k$, et

$$a_n = \begin{cases} a_{n-1} + 1 & \text{si } \operatorname{pgcd}(a_{n-1}, n) = 1 \\ 2n & \text{sinon.} \end{cases}$$

Montrer que la suite $(a_{n+1} - a_n)_{n\geq k}$ a une infinité de termes qui sont des nombres premiers.

Solution de l'exercice 8: Partons d'un entier n tel que $a_n = 2n$. Montrons par récurrence que si p est le plus petit facteur premier de $n-1$, alors pour tout $i \in \{0, \dots, p-2\}$, $a_{n+i} = 2n + i$. En effet, c'est vrai pour $i = 0$, et si c'est vrai pour un certain $i < p-2$, alors

$$\operatorname{pgcd}(n+i+1, 2n+i) = \operatorname{pgcd}(n+i+1, n-1) = \operatorname{pgcd}(i+2, n-1) = 1$$

car $i+2 < p$, et donc $i+2$ est premier avec $n-1$ par définition de p, ce qui conclut la récurrence. De même, $\operatorname{pgcd}(n+p-1, 2n+p-2) = \operatorname{pgcd}(p, n-1) = p \neq 1$, et donc $a_{n+p-1} = 2(n+p-1)$. En particulier,

$$a_{n+p-1} - a_{n+p-2} = 2n + 2p - 2 - (2n + p - 2) = p$$

est premier.

Puisque $a_k = 2k$, avons donc montré qu'il existe une infinité de n satisfaisant $\operatorname{pgcd}(a_{n-1}, n) \neq 1$, et que pour de telles valeurs de n, $a_n - a_{n-1}$ est premier.

Exercice 9 Soit t un entier naturel non-nul. Montrer qu'il existe un entier $n > 1$ premier avec t tel que pour tout entier $k \geq 1$, l'entier $n^k + t$ ne soit pas une puissance (c'est-à-dire qu'il ne soit pas de la forme m^r avec $m \geq 1$ et $r \geq 2$).

Solution de l'exercice 9: Pour que n soit premier avec t, on va le chercher sous la forme $1 + ts$ où s est entier. On aura alors $n^k + t \equiv 1 + t \pmod{s}$. En particulier, si s est divisible par $(t+1)$, alors $n^k + t$ l'est également.

On va d'abord traiter le cas où $t+1$ n'est pas une puissance. Dans ce cas, il suffirait de s'assurer qu'on peut choisir s de telle sorte que $n^k + t$ soit divisible par $t+1$, et que le quotient soit premier avec $t+1$. Pour cela, prenons $s = (t+1)^2$. Alors $n = 1 + t(t+1)^2$, et

$$n^k + t = \underbrace{\sum_{i=1}^{k} \binom{k}{i} t^i (t+1)^{2i}}_{\text{termes divisibles par } (t+1)^2} + 1 + t = (t+1)(a(t+1)+1)$$

pour un certain entier a, donc on a gagné.

Supposons maintenant que $t+1$ soit une puissance : $t+1=m^r$ avec m qui n'est pas une puissance. Si on garde le même n que ci-dessus, on voit que si $n^k+t=b^d$ est une puissance (avec $d\geq 2$), alors $t+1$ est nécessairement une puissance d-ième, et donc d divise r. Ainsi, nous avons une borne sur les d tels que n^k+t est puissance d-ième pour un certain k. On constate alors qu'en remplaçant n par sa puissance r-ième, c'est-à-dire en posant $n=n_0^r$ où $n_0=1+t(t+1)^2$ (ce qui ne change pas le fait que $t+1$ divise n^k+t, que le quotient soit premier avec $t+1$, et que donc $n^k+t=b^d$ implique $d|r$ comme ci-dessus), on arrive à écrire t comme une différence de deux puissances d-ièmes :

$$t=b^d-(n_0^{ke})^d$$

où e est l'entier naturel tel que $r=de$. Cela n'est pas possible car n_0 est grand par rapport à t. Plus précisément, nous avons :

$$t=b^d-(n_0^{ke})^d=(b-n_0^{ke})(b^{d-1}+b^{d-2}n_0^{ke}+\ldots+bn_0^{ke(d-2)}+n_0^{ke(d-1)})\geq n_0>t,$$

contradiction. Donc pour tout k et pour tout d, n^k+t n'est pas une puissance d-ième et nous avons terminé.