Equations fonctionnelles en arithmétique

Martin Rakovsky

Les équations fonctionnelles en théorie des nombres rassemblent le meilleur des deux monde : les raisonnements arithmétiques (divisibilité, étude des nombres premiers) sont utilisés pour enrichir les astuces de substitutions/étude de fonction propres aux équations fonctionnelles.

On distingue principalement trois types d'équations fonctionnelles en théorie des nombres :

- Les équations fonctionnelles faisant intervenir uniquement le caractère discret de $\mathbb{N}$. Malheureusement, ces EF sont des faux-amis : il n'y a pratiquement pas d'arithmétique, le caractère entier des fonctions sert à simplifier certaines équations algébriques, à transformer des inégalités strictes $x > y$ en inégalités larges $x \geqslant y+1$ ou encore que si $x^2+b^2 \leqslant C$, alors a et b prennent un nombre fini de valeurs possibles. Ce genre d'EF est généralement assez prévisible, souvent parce que dans ce cas l'EF donnée en énoncé ressemble "trop" à une EF classique.
- Les équations fonctionnelles ne faisant intervenir que des substitutions et de la divisibilité (et les arguments de taille qui vont avec). Ces EF sont souvent présentées sous la forme $LHS \mid RHS$.
- Les équations fonctionnelles qui font intervenir plus d'arithmétique, et notamment l'étude des nombres premiers. Elles peuvent prendre toutes les formes, y compris les formes du type 2. Donc essayez les idées qui répondent aux deux types.

Nous allons nous occuper dans ce TD d'EF principalement issues du troisième type. Pour des EF du deuxième type, on pensera à regarder le IMO SL 2013 N1 et le Balkan MO 2017 P3. Pour le présent TD, mes conseils sont les suivants :

- Utiliser les arguments de divisibilité habituels : encadrer une expression par deux multiples de n, un carré par deux carrés consécutifs, montrer qu'une différence est divisible par des entiers arbitrairement grands...
- Chercher les valeurs du type $f(p), f(pq), f(p^2), f(pn)$. Substituer un entier naturel par un nombre premier va souvent simplifier l'équation/apporter plus d'infos.
- Dans le cas d'une EF sous la forme $RHS \mid LHS$, ne pas juste chercher à simplifier le RHS. On peut être tenter de s'arranger pour que le RHS soit un nombre très simple. Mais en réalité, travailler pour que le RHS soit divisible par une expression simple suffit amplement. Par exemple, si on a une relation du type $m^2+f(n) \mid mf(m)+n$, substituer m par $f(n)$ permet d'obtenir $f(n) \mid RHS \mid LHS$ et donc $f(n) \mid n$.
- Toujours dans le cas d'un EF sous la forme $RHS \mid LHS$, on peut chercher à rendre le LHS simple, une puissance de p par exemple. Un argument en particulier à avoir sous le coude : si vous avez obtenu $f(p)$ pour tout p, alors le fait que $p \mid n^{p-1}-1$ peut vous permettre de relier p à n, pour peu que l'EF fasse intervenir de la divisibilité.
- Toujours (et encore) dans le cas d'un EF sous la forme $RHS \mid LHS$, une fois que vous avez obtenu la valeur de f pour une inifnité de valeurs, essayez de transformer la divisibilité en $LHS \mid f(a)-a$ avec a fixé et le LHS qui peut prendre une infinité de valeurs.
- Une stratégie se calquant sur plusieurs problèmes où f serait l'identité est d'étudier les diviseurs de $f(n+1)-f(n)$. Si on obtient une contradiction, cela donne $f(n+1)-f(n) = \pm 1$. Merci à Thomas Budzinski qui m'a montré cette technique.
- Dans le cas d'équations fonctionnelles très difficiles, ne pas hésiter à déployer l'artillerie lourde des boîtes noires. Les théorèmes suivants ont déjà vu une EF s'en servir : Dirichlet, LTE, Zsigmondy ou encore "un entier qui est un carré mod p pour tout p est un carré parfait".

Pour d'autres équations fonctionnelles arithmétiques, je vous renvoie à l'excellent cours de Thomas Budzinski donné au groupe D du stage d'été de Valbonne 2022.

1 Exercices

Problème 1. (Canada MO 2017) Soit $f : \mathbb{N}^\star \to \mathbb{N}^\star$ une fonction telle que pour tout entier $n \geq 1$, $f(f(n))$ soit égal au nombre de diviseurs positifs de n. Montrer que si p est un nombre premier, alors $f(p)$ est aussi un nombre premier.

Problème 2. (TST Suisse 201 ?, P1) Trouver toutes les fonctions de $\mathbb{Z}$ dans $\mathbb{Z}$ telles que $f(p) > 0$ pour tout nombre premier p et pour tout p premier et x entier,

$$p \mid (f(x) + f(p))^{f(p)} - x.$$

Problème 3. (USA TSTST 2022, P4) Soit f une fonction de $\mathbb{N}^\star$ dans $\mathbb{N}^\star$ telle que, pour tout couple d'entiers strictement positifs m et n, exactement un seul des entiers

$$f(m+1), \ldots, f(m+f(n))$$

est divisible par n. Montrer que $f(n) = n$ pour une infinité d'entiers n.

Problème 4. (Balkan MO SL 2020 N3) Soit $k \geqslant 2$. Trouver toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que ; pour tous entiers strictements positif $x_1, ..., x_k$, on ait

$$x_1! + ... + x_k! \mid f(x_1)! + ... + f(x_k)!$$

Problème 5. (IMO SL 2019 N4) Soit C un entier naturel non nul. Trouver toutes les fonctions $f \colon \mathbb{N}^* \to \mathbb{N}^*$ telles que, pour tous les entiers a et b de somme $a + b \geqslant C$, l'entier $a + f(b)$ divise $a^2 + bf(a)$.

Problème 6. (EGMO 2022 P2) Déterminer toutes les fonctions de $\mathbb{N}^\star \to \mathbb{N}^\star$ telles que pour tous entiers a et b, on a

1. $f(ab) = f(a)f(b)$
2. Au moins deux des entiers $f(a), f(b)$ et $f(a+b)$ sont égaux.

Problème 7. (IMO SL 2020 N5) Trouver les fonctions $f \colon \mathbb{N}_{\geqslant 1} \mapsto \mathbb{N}_{\geqslant 0}$ vérifiant les deux conditions suivantes :

1. $f(xy) = f(x) + f(y)$ pour tous les entiers $x \geqslant 1$ et $y \geqslant 1$;
2. il existe une infinité d'entiers $n \geqslant 1$ tels que l'égalité $f(k) = f(n-k)$ est vraie pour tout entier k tel que $1 \leqslant k \leqslant n-1$.

On note $\mathbb{N}_{\geqslant 0}$ l'ensemble des entiers supérieurs ou égaux à 0, *et $\mathbb{N}_{\geqslant 1}$ l'ensemble des entiers supérieurs ou égaux à* 1.

Problème 8. (IMO SL 2008 N5) Pour tout entier $n \in \mathbb{N}$, on pose $d(n)$ le nombre de diviseurs positifs de n. Déterminer toutes les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que
(i) $d(f(x)) = x$ pour tout $x \in \mathbb{N}$.
(ii) $f(xy)$ divise $(x-1)y^{xy-1}f(x)$ pour tous $x, y \in \mathbb{N}$.

Problème 9. (EMC 2021 P3 senior) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$x^2 - y^2 + 2y(f(x) + f(y))$$

est un carré parfait pour tous $x, y > 0$.

Problème 10. (SL ELMO 2014/N8) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que :
(i) Les entiers $f(1), f(2), \ldots$ sont premiers entre dans leur ensemble.
(ii) Il existe $N \geq 1$ tel que pour tout $n \geq N$, $f(n) \neq 1$ et pour tous $a, b \in \mathbb{N}^\star$,

$$f(a)^n \mid f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}.$$

2 Solutions

2.1 Canada 2017

Problème 1. (Canada MO 2017) Soit $f : \mathbb{N}^\star \to \mathbb{N}^\star$ une fonction telle que pour tout entier $n \geq 1$, $f(f(n))$ soit égal au nombre de diviseurs positifs de n. Montrer que si p est un nombre premier, alors $f(p)$ est aussi un nombre premier.

Solution 1. Dans la suite, on note $d(n)$ le nombre de diviseurs positifs de n. Si p est premier, on a $f(f(p)) = 2$ par définition. En appliquant f des deux côtés de l'égalité, on voit que $f(2) = d(f(p))$. On veut donc montrer que $f(2) = 2$, ce qui prouvera que $f(p)$ a exactement deux diviseurs et est donc premier. Or, on a aussi $f(2) = d(f(2))$. Or, pour qu'un entier $n \geq 2$ soit égal à son nombre de diviseurs, tous les nombres inférieurs à n doivent diviser n, y compris $n-1$ qui est toujours premier avec n, donc $n-1 = 1$ et $n = 2$. On déduit que $f(2) \in \{1, 2\}$. Si $f(2) = 1$, alors $d(f(p)) = 1$ pour tout p premier, donc $f(p) = 1$ pour p premier, puisque 1 est le seul entier à admettre un seul diviseur. Mais alors

$$1 = f(3) = f(d(2^2)) = f(f(f(2^2))) = d(f(2^2))$$

et l'on déduit que $f(4) = 1$. Mais alors

$$f(f(4)) = f(1) = f(f(2)) = d(2) = 2 \neq d(4)$$

ce qui fournit la contradiction désirée. On a donc bien $f(2) = 2$, ce qui conclut.

2.2 Suisse TST

Problème 2. (TST Suisse 201 ?, P1) Trouver toutes les fonctions de $\mathbb{Z}$ dans $\mathbb{Z}$ telles que $f(p) > 0$ pour tout nombre premier p et pour tout p premier et x entier,

$$p \mid (f(x) + f(p))^{f(p)} - x.$$

Solution 2. Avec $x = p$, on a que p divise $f(p)$ si p impaire. $x = 0$ donne que p divise $f(0)$ pour tout p impaire donc $f(0) = 0$. Alors 2 divise $f(2)^{f(2)}$ donc $f(2)$. Soit q un diviseur premier de $f(p)$ qui n'est pas p (par supposition). Alors avec $x = p$ et la division appliquée pour q on a

$$q \mid (f(p) + f(q))^{f(q)} - p$$

donc q divise p, absurde. Il vient que $f(p)$ est une puissance de p. Modulo p on a donc pour x fixé, par Fermat :

$$x \equiv f(x)^{f(p)} \equiv f(x)$$

donc p divise $f(x) - x$ pour tout p donc $f(x) = x$ pour tout x.

2.3 USA TST 2022

Problème 3. Soit f une fonction de $\mathbb{N}^\star$ dans $\mathbb{N}^\star$ telle que, pour tout couple d'entiers strictement positifs m et n, exactement un seul des entiers

$$f(m+1), \ldots, f(m+f(n))$$

est divisible par n. Montrer que $f(n) = n$ pour une infinité d'entiers n.

Solution 3. Soit $n \geqslant 1$. Pour tout entier $m \geqslant 1$, chacun des deux ensembles

$$\{f(m+1), \ldots, f(m+f(n))\} \quad \text{et} \quad \{f(m+2), \ldots, f(m+1+f(n))\}$$

contient exactement un entier divisible par n. Ainsi, si $n \mid f(m+1)$, aucun des entiers $f(m+2), \ldots, f(m+f(n))$ n'est divisible par n, de sorte que n divise $f(m+1+f(n))$. De même, si n ne divise pas $f(m+1)$, n divise un des entiers $f(m+2), \ldots, f(m+f(n))$, donc n ne divise pas $f(m+1+f(n))$. En conclusion, pour tout entier $m \geqslant 2$, n divise $f(m)$ si et seulement si n divise $f(m+f(n))$. Cela signifie que pour toute paire d'entiers (x, y) supérieurs ou égaux à 2, n divise $f(x)$ et $f(y)$ si et seulement si $f(n)$ divise $x - y$.

Soient maintenant $k \geqslant 1$ un entier et x un entiers tel que $kn \mid f(x)$. Alors kn divise également $f(x+f(kn))$, de sorte que n divise $f(x)$ et $f(x+f(kn))$. On déduit que $f(n)$ divise $f(kn)$ pour tout entier $k \geqslant 1$.

En particulier $f(n)$ divise $f(n)$ et $f(2n)$, donc $f(f(n))$ divise $2n - n = n$. Remarquons ensuite que si n divise $f(n)$, alors il existe un entier k tel que $f(n) = kn$. Mais alors $f(kn) = f(f(n)) \mid n \mid f(n) \mid f(kn)$, de sorte que $f(kn) = f(n)$, donc $n \mid f(n) = f(kn) = f(f(n)) \mid n$ et $f(n) = n$. Ainsi, il suffit de trouver des entiers n tels que $f(n) \mid n$.

D'autre part, puisque $f(f(n))$ divise n, on a en particulier pour tout nombre premier, $f(f(p))$ divise p, donc $f(f(p)) \in \{1, p\}$. Supposons que x soit tel que $f(x) = 1$. Alors pour tout entier $m \geqslant 1$, l'ensemble $\{f(m+1), \ldots, f(m+f(x))\}$ est réduit à $\{f(m+1)\}$, de sorte que x divise $f(m+1)$ pour tout m. En particulier, x divise $f(x) = 1$, donc $x = 1$. Ainsi, $f(p) \neq 1$ et $f(f(p)) \neq 1$ donc $f(f(p)) = p$ pour tout nombre premier p.

Si p divise $f(p)$ pour une infinité de nombres premiers p, alors d'après la discussion précédente, $f(p) = p$ pour une infinité de nombres premiers, ce qui donne le résultat voulu. Sinon, pour tout nombre premier p suffisamment grand, $f(p)$ et p sont premiers entre eux. On a alors $f(p) \mid f(pf(p))$ et $p = f(f(p)) \mid f(pf(p))$, de sorte $pf(p) \mid f(pf(p))$ et $f(pf(p)) = pf(p)$.

Il reste à voir que $pf(p)$ peut prendre une infinité de valeurs différentes. Pour cela, on suppose que l'on a construit k entiers différents de la forme $pf(p)$ et on choisit q un nombre premier sitrictement plus grand que ces k entiers. Alors $qf(q)$ est un bien un entier distincts des k précédents.

f admet donc une infinité de points fixes.

2.4 Balkan MO SL N3

Problème 4. (Balkan MO SL 202 ? N3) Soit $k \geqslant 2$. Trouver toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que ; pour tous entiers strictements positif $x_1, ..., x_k$, on ait

$$x_1! + ... + x_k! \mid f(x_1)! + ... + f(x_k)!$$

Solution 4. Réponse : La seule fonction est la fonction identité.

Soit f une solution éventuelle. En prenant $x_1 = \ldots = x_k = x$, la relation donne que $k \cdot x! \mid k \cdot f(x)!$, ce qui implique que $x! \mid f(x)!$. On déduit que $x \leqslant f(x)$ pour tout entier x strictement positif.

Fixons désormais un nombre premier $p > f(1)$, $x_1 = 1, x_2 = p-1$ et $x_3 = \ldots = x_k = N$ avec $N \geqslant p$. Puisque $f(N) \geqslant N \geqslant p$, $p \mid f(N)!$ et $p \mid N!$. De plus, d'après le théorème de Wilson, $p \mid (p-1)! + 1$. Ainsi, la relation de l'énoncé implique que

$$p \mid 1 + (p-1)! + (k-2)N! \mid f(1)! + f(p-1)! + (k-2)f(N)!$$

Comme p divise $f(N)!$, on a $p \mid f(1)! + f(p-1)!$. Mais $p > f(1)$ donc p ne divise pas $f(1)!$. Donc p ne divise pas non plus $f(p-1)!$. On a donc $f(p-1) \leqslant p-1$ et $f(p-1) = p-1$ pour tout entier $p > f(1)$.

Prenons alors n un entier strictement positif et $p > f(1)$ un nombre premier. On pose $x_1 = n, x_2 = \ldots = x_k = p-1$. La relation de l'énoncé donne

$$n! + (k-1) \cdot (p-1)! \mid f(n)! + (k-1) \cdot f(p-1)! = f(n)! + (k-1) \cdot (p-1)!.$$

Mais alors

$$n! + (k-1) \cdot (p-1)! \mid f(n)! + (k-1) \cdot (p-1)! - (n! + (k-1) \cdot (p-1)!) = f(n)! - n!.$$

Cette relation de divisibilité étant vraie pour tout nombre premier $p > f(1)$, le nombre $f(n)! - n!$ admet une infinité de diviseurs, il est donc nul. On a bien $f(n) = n$ pour tout entier n.

Réciproquement, on vérifie que la fonction f vérifie la relation de récurrence.

2.5 IMO SL 2019 N4

Problème 5. Soit C un entier naturel non nul. Trouver toutes les fonctions $f\colon \mathbb{N}^* \to \mathbb{N}^*$ telles que, pour tous les entiers a et b de somme $a+b \geqslant C$, l'entier $a+f(b)$ divise $a^2+bf(a)$.

Solution 5. Tout d'abord, toute fonction linéaire strictement croissante est solution. En effet, pour tout entier $k \geqslant 1$, l'entier $a+kb$ divise bien $a^2+b\times(ka) = a(a+kb)$. Réciproquement, montrons que toute solution est une fonction linéaire (qui sera strictement croissante, puisque à valeurs dans $\mathbb{N}^*$).

Notons d'abord que si a et b sont des entiers tels que $a+b \geq C$, alors en substituant a par 1, on obtient que pour tout $b \geq C$:

$$1+f(b) \mid 1+bf(1)$$

soit $1+f(b) \leq 1+bf(1)$ donc $f(b) \leq bf(1)$ pour tout entier $b \geq C$.

De plus, si a et b vérifient que $a+b \geq C$:

$$a+f(b) \mid a^2+bf(a)-(a+f(b))(a-f(b)) = f(b)^2+bf(a)$$

Soit $b \geq 1$ un entier. On choisit un entier $n \geq 1$ tel que $b^n - f(b) \geq C$. On pose alors $a = b^n - f(b)$ pour obtenir que

$$b \mid b^n = b^n - f(b) + f(b) \mid f(b)^2 + bf(b^n - f(b))$$

On déduit que b divise $f(b)^2$ pour tout entier strictement positif b.

En particulier si p est un nombre premier, p divise $f(p)$. On montre à présent que $f(p) = pf(1)$ pour une infinité de nombres premiers p.

Soit p un nombre premier strictement supérieur à $f(1)$ et à C. Alors en remplaçant a par p et b par 1 on trouve

$$p+f(1) \mid p^2+f(p)$$

Or p est premier avec $p+f(1)$ et p divise chacun des termes p^2 et $f(p)$ donc $p(p+f(1))$ divise $p^2+f(p)$. On déduit $p^2+pf(1) \leq p^2+f(p)$ soit $pf(1) \leq f(p)$. Ceci combiné avec l'inégalité $f(p) \leq pf(1)$ si p est suffisamment grand donne $f(p) = pf(1)$ pour une infinité de nombres premiers p.

Soit a un entier et soit p un nombre premier tel que $f(p) = pf(1)$ et tel que p et $a+pf(1)$ soient premiers entre eux (la deuxième condition s'obtient pour en prenant p suffisamment grand). Alors en substituant b par p, on obtient

$$a+pf(1) \mid a^2+pf(a)-a(a+pf(1)) = p(f(a)-af(1))$$

Or $a+cp$ est premier avec p donc $a+pf(1)$ divise $f(a)-af(1)$. Mais cette relation de dvisibilité est vraie pour une infinité de nombres premiers p. On déduit que $f(a) = af(1)$ pour tout entier a. f est bien linéaire strictement croissante.

Solution alternative n° 1

On présente une autre façon de conclure une fois que l'on a montré que p divise $f(p)$ pour tout nombre premier p.

Soit p un nombre premier. On dispose d'un entier c_p tel que $f(p) = c_p p$. Etant donné que pour p suffisement grand, $f(p) \leq pf(1)$, la suite (c_p) est bornée. Donc il existe un entier c et une infinité de nombres premiers p tels que $c_p = c$.

SOit alors a un entier et p un nombre premier suffisamment grand tel que $f(p) = cp$ et p soit premier avec a. en particulier, p est premier avec $a+cp$. En substituant b par p, on trouve

$$a+cp \mid a^2+pf(a)-a(a+cp) = p(f(a)-ca)$$

Mais comme p est premier avec $a+cp$, on déduit que $a+cp \mid f(a)-ca$. Comme cette divisibilité est vrai pour une infinité d'entiers p, on obtient que $f(a) = ca$ pour tout entier a. En remplaçant a par 1, on trouve $c = f(1)$ donc f est linéaire strictement croissante.

Solution alternative n° 1

Une façon de conclure à partir de l'inégalité $1+f(b) \mid 1+bf(1)$ est d'utiliser le théorème de Dirichlet : il existe une infinité d'entiers b tels que $1+bf(1)$ est premier. Pour ces entiers b, on trouve que $1+f(b) = 1+bf(1)$, ce qui donne une infinité d'entiers b tels que $f(b) = bf(1)$. On peut alors conclure comme dans la solution 1.

2.6 EGMO 2022 P2

Problème 6. (EGMO 2022 P2) Déterminer toutes les fonctions de $\mathbb{N}^\star \to \mathbb{N}^\star$ telles que pour tous entiers a et b, on a

1. $f(ab) = f(a)f(b)$
2. Au moins deux des entiers $f(a), f(b)$ et $f(a+b)$ sont égaux.

Solution 6. Si f est constante, $f = 1$ d'après la première équation, et il s'agit bien d'une solution.

Si f est non constante égale à 1, on note $S = \{x, f(x) > 1\}$. On note que 1 n'est pas dans S d'après la première relation. Au vu de la première relation, si $x \in S$, l'un de ses diviseurs l'est aussi, donc l'élément minimal de S est un nombre premier que l'on note p. Nous allons alors montrer que $f(x) = f(p)^{v_p(n)}$. (On vérifie bien qu'une telle fonction est solution). On vérifie que $f(p^\alpha) = f(p)^\alpha$, et puisque $f(n) = \prod f(p_i)^{\alpha_i}$ si $n = \prod p_i^{\alpha_i}$, il suffit de montrer que $f(q) = 1$ pour tout premier $q \neq p$.

Soit alors $q \in S$ un nombre premier. Il faut utiliser la deuxième relation pour rassembler ces informations. Pour cela, on va créé un multiple de q qui soit proche d'une puissance de p. D'après le petit théorème de Fermat, $q \mid p^{q-1} - 1$, donc $f(p^{q-1} - 1) > 1$. Or deux des nombres $f(1) = 1, f(p^{q-1} - 1)$ et $f(p^{q-1}) = f(p)^{q-1}$ sont égaux. Il vient que $f(p^{q-1} - 1) = f(p)^{q-1}$.

D'autre part, on vérifie que $f(p+1) = 1$ (ses facteurs premiers sont inférieurs à p) donc $f(p^2+p) = f(p)$. Ainsi, $f(p^2 + p + 1) = 1$ ou $f(p)$ d'après la deuxième condition. Par récurrence sur k, on montre que $f(p^k + p^{k-1} + \ldots + p + 1) \in \{1, f(p), \ldots, f(p)^{k-1}\}$. Or,

$$f(p^{q-2} + \ldots + p + 1) = \frac{f(p^{q-1} - 1)}{f(p-1)} = f(p)^{q-1},$$

ce qui est absurde. Cela conclut.

2.7 IMO 2020 N5

Problème 7. Trouver les fonctions $f\colon \mathbb{N}_{\geqslant 1} \mapsto \mathbb{N}_{\geqslant 0}$ vérifiant les deux conditions suivantes :

1. $f(xy) = f(x) + f(y)$ pour tous les entiers $x \geqslant 1$ et $y \geqslant 1$;
2. il existe une infinité d'entiers $n \geqslant 1$ tels que l'égalité $f(k) = f(n-k)$ est vraie pour tout entier k tel que $1 \leqslant k \leqslant n-1$.

On note $\mathbb{N}_{\geqslant 0}$ l'ensemble des entiers supérieurs ou égaux à 0*, et $\mathbb{N}_{\geqslant 1}$ l'ensemble des entiers supérieurs ou égaux à* 1.

Solution 7. Les fonctions recherchées sont les fonctions de la forme $f\colon n \mapsto cv_p(n)$, où c est un entier naturel, p est un nombre premier, et $v_p(n)$ et la valuation p-adique de n. Tout d'abord, il est clair que ces fonctions sont bien solutions du problème.

Réciproquement, soit f une solution non nulle du problème. On dit qu'un entier n est *joli* si l'égalité $f(k) = f(n-k)$ est vraie pour tout entier $k \leqslant 1$. Remarquons que tout diviseur d'un joli entier est joli. En effet, si d divise un joli entier $n = ad$, alors

$$f(k) = f(ak) - f(a) = f(n-ak) - f(a) = f(a(d-k)) - f(a) = f(d-k)$$

pour tout entier $k \leqslant d-1$.

En outre, la condition 1 signifie que $f\left(\prod_i p_i^{\alpha_i}\right) = \sum_i \alpha_i f(p_i)$ pour toute décomposition en produit de facteurs premiers. Il s'agit donc de démontrer qu'il existe au plus un nombre premier p pour lequel $f(p) > 0$. On considère alors le plus petit entier p tel que $f(p) > 0$. La formule ci-dessus indique que p est premier, et on pose $c = f(p)$.

S'il existe un joli entier $n \geqslant p$ que p ne divise pas, posons $n = pq + r$, avec q entier et $1 \leqslant r \leqslant p-1$. Puisque n est joli, on sait que $f(r) = f(n-pq) = f(pq) \geqslant f(p) > 0$, en contradiction avec la définition de p. Ainsi, tout entier joli est de la forme ap^b avec b entier et $1 \leqslant a \leqslant p-1$. Réciproquement, puisqu'il existe une infinité d'entiers jolis et que a ne peut prendre qu'un nombre fini de valeurs, toute puissance de p divise un joli entier, et est donc elle-même jolie.

Par conséquent, pour tout nombre premier q distinct de p, l'entier p^{q-1} est joli. Puisque q divise $p^{q-1}-1$, on en déduit en particulier que $0 = f(1) = f(p^{q-1}-1) \geqslant f(q)$, ce qui conclut.

Solution alternative :

Une fois acquis le fait que tout entier joli est de la forme ap^b, avec b entier et $1 \leqslant a \leqslant p-1$, et que tout diviseur d'un entier joli est joli, on peut aussi procéder comme suit.

Supposons qu'il existe un nombre premier $q \neq p$ pour lequel $f(q) > 0$, et soit q le plus petit tel nombre premier. On considère alors le plus petit entier joli $n > q$, puis on écrit n sous la forme $n = ap^b = uq + v$, avec u entier et $0 \leqslant v \leqslant q-1$.

Puisque $n > q > p$, on sait que $b \geqslant 1$, donc que p divise n, et comme q ne divise pas n, on sait que $v \geqslant 1$. Dans ces conditions, $f(v) = f(uq) > 0$, et la minimalité de q indique que p divise v. Mais alors p divise aussi $uq = n - v$, et p est premier avec q, donc p divise u. On en déduit que $n > pq$, donc que le joli entier n/p satisfait lui aussi l'inégalité $n/p > q$, en contradiction avec la minimalité de n. Notre supposition est ainsi invalide, ce qui conclut.

2.8 IMO SL 2008 N5

Problème 8. (IMO SL 2008 N5) Pour tout entier $n \in \mathbb{N}$, on pose $d(n)$ le nombre de diviseurs positifs de n. Déterminer toutes les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que
(i) $d(f(x)) = x$ pour tout $x \in \mathbb{N}$.
(ii) $f(xy)$ divise $(x-1)y^{xy-1}f(x)$ pour tous $x, y \in \mathbb{N}$.

Solution 8. Réponse : $f(n) = \displaystyle\prod_{i=1}^{r} p_i^{p_i^{\alpha_i}-1}$ lorsque $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ et $f(1) = 1$.

Tout d'abord, on vérifie qu'une telle solution fonctionne bien.

Soit maintenant f une solution du problème. La première condition donne que $f(1) = 1$. D'autre part, la première condition donne que f est injective. Enfin, la première condition donne que $f(2)$ est un nombre premier.

En appliquant toujours la première condition à $x = p$, on déduit que $f(p)$ admet exactement p diviseurs. Au vu de la formule sur le nombre de diviseurs, cela implique que $f(p)$ est une puissance d'un nombre premier, disons $f(p) = q^{p-1}$. En posant $x = 2, y = p$ dans l'hypothèse 2, on a $f(2p) \mid p^{2p-1}f(2)$, tandis qu'en $x = p, y = 2$, on trouve $f(2p) \mid (p-1)2^{2p-1}q^{p-1}$. En particulier, si p est impair et si $q \neq p$, p est premier avec $(p-1)2^{2p-1}q^{p-1}$, donc

$$f(2p) \mid \gcd(p^{2p-1}f(2), (p-1)2^{2p-1}q^{p-1}) \mid \gcd(f(2), (p-1)2^{2p-1}q^{p-1}) \mid f(2).$$

Donc $f(2p)$ est un diviseur de $f(2)$ qui est premier. Comme $d(f(2p)) = 2p$, $f(2p) > 1$ donc $f(2p) = f(2)$ et par injectivité $p = 1$, ce qui est absurde. Donc $f(p) = p^{p-1}$ si p est impair.

On calcule désormais $f(2)$: en posant $x = 2, y = 3$ et $x = 3, y = 2$, on trouve que $f(6)$ divise $2^6 f(3) = 2^6\$cdot 3^2$ et $3^5 f(2)$. Si $f(2)$ est impair, alors $f(6) \mid 3^2$. Or $f(6)$ admet 6 diviseurs. Donc $f(2)$ un nombre premier pair et $f(2) = 2$.

On prouve à présent que les seuls facteurs premiers de $f(n)$ sont des facteurs premiers de n. Notons $n = \prod p_i^{\alpha_i}$. On suppose que p_1 est le plus petit diviseur premier de n et on suppose qu'existe A divisant $f(n)$ et distinct des p_i. En posant $x = p_1$ et $y = n/p$, on trouve que $A \mid f(n) \mid (p_1 - 1)(n/p_1)^{n-1}p_1^{p_1-1}$. Donc $A \mid p_1 - 1$. Autrement dit, si $f(n) = AB$, avec d premier avec A et B ayant ses facteurs premiers parmi ceux de n, on a

$$d(A)d(B) = d(AB) = d(f(n)) = n.$$

Donc $d(A)$ divise n, mais ses éventuels facteurs premiers sont tous inférieurs à $p_1 - 1$. On déduit que $d(A) = 1$ et $A = 1$. Ceci donne le résultat annoncé.

Ceci implique directement que $f(p^\alpha)$ est une puissance de p. L'hypothèsé 1 donne alors que $p^\alpha = df(p^\alpha)) = v_p(f(p^\alpha)) + 1$, donc $f(p^\alpha) = p^{p^\alpha - 1}$.

On passe à la forme générale de $f(n)$. On écrit $n = \prod p_i^{\alpha_i}$ et $f(n) = \prod p_i^{\beta_i}$. En posant $x = p_i^{\alpha_i}$ et $y = n/x$, on a

$$p_i^{\beta_i} \mid f(n) \mid (p_i^{\alpha_i} - 1)y^{n-1}p_i^{p_i^{\alpha_i}-1}.$$

Donc $p_i^{\beta_i} \mid p_i^{p_i^{\alpha_i}-1}$ donc $\beta_i \leqslant p_i^{\alpha_i} - 1$. Mais l'hypothèsé 1 permet de saturer cette inégalité :

$$p_1^{\alpha_1} \dots p_r^{\alpha_r} \geqslant (\beta_1 + 1) \dots (\beta_r + 1) = d(f(n)) = n = \prod p_i^{\alpha_i}.$$

Ainsi $\beta_i = p_i^{\alpha_i}$, ce qui conclut.

2.9 EMC 2021

Problème 9. (EMC 2021 P3 senior) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que

$$x^2 - y^2 + 2y(f(x) + f(y))$$

est un carré parfait pour tous $x, y > 0$.

Solution 9. Soit f une solution. Pour $x = y = p$ un nombre premier, on voit que $4pf(p)$ est un carré pour tout p, donc $pf(p)$ est un carré pour tout p et $p \mid f(p)$.

On déduit en posant $x = p$ dans l'hypothèse que $-y^2 + 2yf(y)$ est un carré modulo p, et ce pour tout p. Ceci implique que $-y^2 + 2yf(y)$ est un carré parfait. On pose c_y l'entier tel que $c_y^2 = -y^2 + 2yf(y)$. En réinjectant dans l'hypothèse et en prenant $x = 1$, on a

$$1 + 2yf(1) + c_y^2$$

qui est un carré parfait strictement plus grand que c_y^2. Ainsi, $1+2yf(1)+c_y^2 \geqslant (c_y+1)$, soit $yf(1) \geqslant c_y$, ce qui donne $y^2 f(1)^2 \geqslant c_y^2$, et finalement

$$f(y) \leqslant \frac{f(1)^2 + 1}{2} y.$$

Ainsi, $\frac{f(p)}{p}$ ne peut prendre qu'une nombre fini de valeurs, comprises entre 1 et $\frac{f(1)^2+1}{2}$. Le principe des tiroirs infini, il existe donc un entier a et une infinité de nombres premierrs p tels que $f(p) = ap$.

On remplace x par un tel p dans l'hypothèse et on trouve que

$$p^2 - y^2 + 2yap + 2yf(y) = (p + ya)^2 - y^2 - y^2a^2 + 2yf(y)$$

est un carré pour tout nombre premier p. En posant $D = -y^2 - y^2a^2 + 2yf(y)$, on trouve que $(p + ya)^2 - D$ est un carré pour une infinité de p, ce qui implique (puisque la différence entre deux carrés consécutifs est plus grand que D à partir d'un certain rang) que $D = 0$. Donc $f(y) = \frac{a^2+1}{2} y$. En remplaçant y par p, on trouve que $a = 1$. Ainsi, $f(y) = y$ pour tout y, et c'est bien une solution de l'équation.

2.10 ELMO SL N8

Problème 10. (SL ELMO 2014/N8) Déterminer toutes les fonctions $f : \mathbb{N}^\star \to \mathbb{N}^\star$ telles que :

(i) Les entiers $f(1), f(2), \ldots$ sont premiers entre dans leur ensemble.

(ii) Il existe $N \geq 1$ tel que pour tout $n \geq N$, $f(n) \neq 1$ et pour tous $a, b \in \mathbb{N}^\star$,

$$f(a)^n \mid f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}.$$

Solution 10. Soit f une solution. Comme les valeurs de f sont premières entre elles dans leur ensemble, si f est constante, elle égale 1, ce qui est exclu.

Avec $a = 1$, on voit que $f(1)^n | f(b+1) - f(b)$ pour tout $b \geq 1$ et tout n assez grand. Comme f est non constante, il existe b tel que $f(b+1) \neq f(b)$. Il s'ensuit que $f(1) = 1$.

Soit $a \geq 2$, il existe un $t \geq 0$ tel que $f(1 + (t+1)a) \neq f(1 + ta)$ (car, pour t assez grand, $f(1+ta) \neq 1 = f(1)$) : soit $b = 1 + ta$. Pour tout $n \geq 1$ assez grand, $f(a)^n | f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}$.

Soit p un nombre premier divisant $f(a)$. Alors il existe un $l \geq 1$ tel que $p | f(a+b)^{a^l} - f(b)^{a^l}$. Pour $n > l$, par LTE, la valuation p-adique de $f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}$ est $v_p(a^{n-1-l}) + C$ pour une certaine constante C qui ne dépend que de f, a, b, l (mais pas de n).

Donc pour $n > l$ assez grand, $v_p(a^{n-1-l}) + C \geq v_p(f(a)^n)$, donc $(n-1-l)v_p(a) + C \geq n v_p(f(a))$, d'où $v_p(f(a)) \leq v_p(a)$.

Par conséquent, pour tout $a \geq 1$, $f(a)|a$.

En particulier, si a est premier, $f(a)$ vaut 1 ou a, et est égal à a sauf pour un nombre fini de nombres premiers.

Soit a un nombre premier tel que $f(a) = a$: pour tout $b \geq 1$ et tout n assez grand, $a^n | f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}$. En particulier, $f(a+b) \equiv f(b)[a]$: ainsi, la classe de congruence de $f(b)$ modulo a ne dépend que de b modulo a.

On va montrer que f est l'identité. Soit $u \geq 2$, soit P l'ensemble fini des nombres premiers p tels que $p \leq u$ ou $f(p) = 1$. Supposons qu'il existe un nombre premier $q \notin P$ et un entier n tels que $q | n - u$ et $f(n) = n$.

Alors $q | f(n) - f(u)$, et donc $q | n - f(u)$, d'où $q | u - f(u)$. Comme $0 \leq u - f(u) \leq u < q$, on en déduit que $f(u) = u$.

On propose trois méthodes, de la plus élémentaire à la moins élémentaire, d'exhiber un tel couple (q, n).

<u>Première méthode</u> (complètement élémentaire) :

Soit Π le produit des nombres premiers de P, et soit $N \geq 1$ tel que pour tout $p \in P$, p^N ne divise pas $u - 1$.

Supposons que $n > \Pi^N + u$ soit congru à 1 modulo Π^N et tel que $f(n) = n$. Alors, si $p \in P$, $v_p(n-u) < N$, et $n - u > \Pi^N$, de sorte que $n - u$ possède un diviseur premier $q \notin P$, et on a gagné.

Soit n un produit de nombres premiers deux à deux distincts, tous hors de P. Alors, si $p|n$ est un diviseur premier, $n \equiv p[p]$ et $f(p) = p$, donc $p | f(n) - f(p)$, d'où $p | f(n)$. Comme $f(n)|n$, on en déduit que $f(n) = n$.

Comme il existe une infinité de nombres premiers, il existe une progression arithmétique C de raison Π^N et de premier terme premier à Π et contenant une infinité de nombres premiers. En prenant pour n le produit de $\varphi(\Pi^N)$ premiers $q \in C$ tels que $q > \Pi^N + u$, n convient.

<u>Deuxième méthode</u> (il y a des prérequis, mais ils sont élémentaires et relativement classiques) :

On reprend les notations et le raisonnement de ce qui précède : on cherche à construire un entier $n > \Pi^N + u$ congru à 1 modulo Π^N tel que $f(n) = n$.

Il est connu (du moins, classique et relativement élémentaire) que si Φ_{Π^N} est le Π^N-ième polynôme cyclotomique, il existe une infinité de nombres premiers n divisant une valeur de Φ_{Π^N}, et ceux qui ne sont pas dans P sont congrus à 1 modulo Π^N et vérifient $f(n) = n$. On peut en choisir un qui est strictement supérieur à $\Pi^N + u$.

<u>Troisième méthode</u> (utilise un théorème relativement classique, mais dont aucune démonstration accessible au niveau olympique n'est connue) :

Soit $q \notin P$ premier : alors $f(q) = q$. D'après le théorème de Dirichlet, il existe un nombre premier $p > u + q$ congru à u modulo q tel que $f(p) = p$. Alors le couple (q, p) convient.

Ainsi, l'identité est la seule solution potentielle. Réciproquement, l'identité vérifie la première condition et si $a, b \geq 1$ et $n \geq 2$, alors par LTE, pour tout nombre premier $p|a$, $v_p((a+b)^{a^{n-1}} - b^{a^{n-1}}) \geq v_p(a) + v_p(a^{n-1}) = v_p(a^n)$, donc $a^n|(a+b)^{a^{n-1}} - b^{a^{n-1}}$, et donc l'identité est solution.