DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Exercices

AUTEUR : Margaret BILU
STAGE : Montpellier 2014

Arithmétique de base

Notions abordées : divisibilité, nombres premiers, décomposition en facteurs premiers, pgcd, ppcm, algorithme d'Euclide, valuations p-adiques, formule de Legendre, théorème de Bézout, lemme de Gauss.

Pour des détails, cf polycopié d'Arithmétique sur le site `www.animath.fr`

0.0.1 Exercices

Exercice 1 Montrer que pour tout $n \in \mathbb{Z}$, $n^2 + n$ est divisible par 2.

Exercice 2 Trouver les valeurs de $n \in \mathbb{N}$ pour lesquelles $13^n - 11^n$ est premier.

Exercice 3

1. Trouver les x dans $\mathbb{Z}$ tels que $x - 1$ divise $x - 3$
2. Trouver les x dans $\mathbb{Z}$ tels que $x + 2$ divise $x^2 + 3$.

Exercice 4 Montrer que la fraction $\frac{21n+4}{14n+3}$ est irréductible pour tout $n \in \mathbb{N}$.

Exercice 5 Montrer que 6 divise $n^3 - n$.

Exercice 6 Soit p un nombre premier supérieur ou égal à 5. Montrer que 24 divise $p^2 - 1$.

Exercice 7 Soient a et b des entiers premiers entre eux. Montrer que ab et $a + b$ sont premiers entre eux.

Exercice 8 On choisit $n+1$ entiers compris entre 1 et $2n$. Montrer que parmi eux il y en a deux qui sont premiers entre eux.

Exercice 9 Soient p premier et $k \in \{1, \dots, p-1\}$. Montrer que $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ est divisible par p.

Exercice 10 On appelle n-ième nombre de Fermat l'entier $F_n = 2^{2^n} + 1$. Montrer que les nombres de Fermat sont premiers entre eux deux à deux.

Exercice 11 Pour tout $n > 1$, trouver n entiers consécutifs non premiers.

Exercice 12 Déterminer le pgcd de tous les nombres de la forme

$$(a-b)(b-c)(c-d)(d-a)(b-d)(a-c)$$

où a, b, c, d parcourent $\mathbb{Z}$.

Exercice 13 Soient a et b deux entiers naturels premiers entre eux. Démontrer que pour tout entier naturel n tel que $n > ab$, il existe deux entiers naturels x et y tels que $n = ax + by$.

0.0.2 Solutions

Solution de l'exercice 1 Première méthode : n et n^2 ont la même parité, donc leur somme est paire.

Deuxième méthode : en factorisant on obtient $n^2 + n = n(n+1)$. Or parmi deux entiers consécutifs, il y en a forcément un qui est pair, donc leur produit est pair.

Solution de l'exercice 2 $13^n - 11^n$ est toujours pair, donc il suffit de vérifier quand il est strictement plus grand que 2. Montrons par récurrence que c'est le cas dès que $n \geqslant 2$. En effet, $13^2 - 11^2 = 169 - 121 = 48 > 2$. Supposons que pour un certain n, $13^n - 11^n > 2$. Alors $13^{n+1} = 13 \times 13^n > 13(11^n + 2) > 11(11^n + 2) > 11^{n+1} + 2$, ce qui conclut. Ainsi, il reste à regarder les cas $n = 0$ et $n = 1$. On a $13^0 - 11^0 = 0$ et $13^1 - 11^1 = 2$, donc la seule solution est $n = 1$.

Solution de l'exercice 3

1. $x - 1$ divise $x - 3$ si et seulement si $x - 1$ divise $x - 3 - (x - 1)$, donc si et seulement si $x - 1$ divise -2. Ainsi, $x - 1$ appartient à l'ensemble $\{-2, -1, 1, 2\}$, c'est-à-dire que $x \in \{-1, 0, 2, 3\}$.
2. $x+2$ divise x^2+3 si et seulement si $x+2$ divise $(x^2+3)-x(x+2) = -2x+3$, si et seulement si $x + 2$ divise $-2x + 3 + 2(x + 2) = 7$. Donc $x + 2$ appartient à l'ensemble $\{-7, -1, 1, 7\}$, c'est-à-dire que $x \in \{-9, -3, -1, 5\}$.

Solution de l'exercice 4 Nous allons calculer le pgcd de $21n + 4$ et de $14n + 3$ en effectuant un algorithme d'Euclide.

$$\begin{aligned} 21n + 4 &= (14n + 3) \times 1 + (7n + 1) \\ 14n + 3 &= (7n + 1) \times 2 + 1 \end{aligned}$$

Donc pour tout n, le numérateur et le dénominateur sont premiers entre eux, donc la fraction est irréductible.

Solution de l'exercice 5 On factorise : $n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1)$. Parmi trois entiers consécutifs, il y en a nécessairement un divisible par 2 et un divisible par 3. Donc $n^3 - n$ est divisible par 2 et par 3, et par conséquent également par le ppcm de 2 et de 3, c'est-à-dire 6.

Solution de l'exercice 6 On factorise encore : $p^2 - 1 = (p - 1)(p + 1)$. Nous savons que p est premier, et qu'il est supérieur à 5 : il est donc impair et non divisible par 3. Ainsi, $p-1$ et $p+1$ sont tous les deux pairs, et l'un d'eux doit être divisible par 3. Mieux : parmi deux nombres pairs consécutifs il y en a un qui est divisible par 4 : ainsi, $(p - 1)$ ou $(p + 1)$ est divisible par 4. Finalement, $p^2 - 1$ est divisible par 3 et par $2 \times 4 = 8$, donc il est divisible par 24.

Solution de l'exercice 7 Soit d un diviseur commun de ab et $a+b$. Alors d divise $ab-a(a+b) = -a^2$, et de même, d divise $ab - b(a + b) = -b^2$. d est donc un diviseur commun de a^2 et b^2. Or si a et b sont premiers entre eux, a^2 et b^2 le sont aussi, donc $d = 1$.

Solution de l'exercice 8 Si on choisit $n + 1$ entiers dans $\{1, \ldots, 2n\}$, il y en aura forcément deux qui seront consécutifs : ces deux-là seront premiers entre eux.

Solution de l'exercice 9 On écrit $p! = \binom{p}{k} \times k!(p-k)!$. Nous savons que p divise $p!$. D'autre part, puisque $k \in \{1, \ldots, p - 1\}$ et que p est premier, $k!$ et $(p - k)!$ n'ont que des facteurs premiers inférieurs strictement à p, donc sont premiers avec p. Ainsi, p divise le côté droit de l'égalité ci-dessus, et est premier avec $k!(p - k)!$, donc par le lemme de Gauss il divise $\binom{p}{k}$.

Attention : c'est faux si p n'est pas premier. Par exemple $\binom{4}{2} = 6$ n'est pas divisible par 4.

Solution de l'exercice 10 On montre par récurrence que pour tout $n \geqslant 0$, $F_{n+1}-2 = F_n F_{n-1} \dots F_0$. Pour l'initialisation, on a bien $F_1 - 2 = 2^2 - 1 = 3 = F_0$. Supposons que la relation à prouver est vraie au rang n. Alors

$$F_{n+1} - 2 = 2^{2^{n+1}} - 1 = \left(2^{2^n} + 1\right)\left(2^{2^n} - 1\right) = F_n(F_n - 2)$$

donc par hypothèse de récurrence on a bien $F_{n+1} - 2 = F_n F_{n-1} \dots F_0$.

Un diviseur commun de F_{n+1} et d'un des F_i précédent diviserait $F_{n+1} + F_0 \dots F_n = 2$. Ne pouvant être égal à 2 car tout nombre de Fermat est impair, il est nécessairement égal à 1. Ainsi, tout terme de la suite des nombres de Fermat est premier avec tous les précédents, ce qui implique que deux nombres de Fermat distincts sont premiers entre eux.

Note : les nombres de Fermat avaient été introduits par Fermat, qui conjecturait qu'ils étaient tous premiers...conjecture infirmée un siècle après par Euler, qui montra que déjà F_5 n'est pas premier. Actuellement nous ne savons toujours pas s'il existe un nombre de Fermat premier autre que $F_0, \dots, F_4$.

Solution de l'exercice 11 Fixons un entier N et regardons ce que nous pouvons dire des diviseurs des entiers successifs situés après N.

$$N \quad N+1 \quad N+2 \quad N+3 \quad \dots \quad N+k \quad \dots$$

Nous ne savons rien sur $N + 1$, si ce n'est qu'il est premier avec N. En revanche, si jamais N est pair, nous savons à coup sûr que $N + 2$ est pair (de même que tous les nombres de la forme $N + 2i$). Si N est multiple de 3, alors $N + 3$ sera nécessairement divisible par 3. Plus généralement, pour tout entier k, si N est divisible par k, $N+k$ l'est aussi. Pour avoir n entiers consécutifs non premiers, il nous faut imposer des conditions sur N de sorte à fournir des diviseurs aux n nombres consécutifs $N + 2, N + 3, \dots, N + (n + 1)$. Il suffit donc que N soit divisible par tous les nombres entre 2 et $n+1$; en choisissant $N = (n+1)!$, nous avons terminé.

Solution de l'exercice 12 Si on calcule le produit en question pour $a = 0, b = 1, c = 2, d = 3$, on trouve -12 donc le pgcd en question divise nécessairement $12 = 3 \times 4$. Réciproquement, nous allons montrer que ce pgcd est 12, en montrant que tous les nombres de cette forme sont divisibles par 3 et par 4.

Un entier n divise la différence entre deux des entiers parmi a, b, c, d si ces entiers ont le même reste dans la division euclidienne par n. Puisqu'il n'y a que 3 restes possibles modulo 3, il y a forcément deux entiers parmi a, b, c, d qui ont le même reste. Tous les produits considérés dans l'énoncé sont donc divisibles par 3.

Regardons maintenant les restes modulo 4 : il y a alors deux cas à considérer. S'il existe deux entiers parmi a, b, c, d qui ont le même reste dans la division euclidienne par 4, la différence entre ces deux entiers sera divisible par 4. Si a, b, c, d ont tous des restes différents modulo 4, cela veut dire que les 4 restes possibles dans la division euclidienne par 4 sont représentés. Ainsi, il y a parmi a, b, c, d deux entiers pairs et deux entiers impairs. La différence entre deux entiers de même parité étant paire, nous avons montré que dans ce cas aussi tous les produits considérés sont divisibles par $2 \times 2 = 4$.

Solution de l'exercice 13 On sait par le théorème de Bézout qu'il existe des entiers u et v tels que $au + bv = 1$. En multipliant cela par n, on obtient

$$a(un) + b(vn) = n.$$

Le problème est que un et vn ne sont a priori pas tous les deux positifs. Au contraire, au vu de l'identité $au + bv = 1$ l'un d'eux doit être négatif et l'autre positif. Supposons par exemple que u est positif et v négatif. L'astuce sera donc d'additionner quelque chose à nv, et de soustraire quelque chose à nu pour compenser. Plus précisément, pour tout entier k, on peut écrire

$$a(un - bk) + b(vn + ak) = n.$$

Reste à voir s'il existe k tel que $vn + ak$ et $un - bk$ sont tous les deux positifs. Cela implique

$$\frac{-vn}{a} \leqslant k \leqslant \frac{un}{b}.$$

Nous devons donc vérifier s'il existe un entier entre $\frac{un}{b}$ et $-\frac{vn}{a}$. Or

$$\frac{un}{b} - \left(-\frac{vn}{a}\right) = \frac{una + vnb}{ab} = \frac{n}{ab} > 1.$$

Entre deux nombres à distance strictement plus grande que 1 il existe nécessairement au moins un entier, on peut donc choisir k de telle sorte que $vn + ak$ et $un - bk$ soient tous les deux positifs.