Arithmétique

Définition Pour $n, m \in \mathbb{N}$, on dit que n divise m, ce que l'on note $n \mid m$, s'il existe $k \in \mathbb{N}$ tel que $m = kn$.
On dit que $p \in \mathbb{N}$ est premier si $p \neq 1$ et si les seuls diviseurs de p sont 1 et lui-même.

Exercice 1 Soient $a, b, c \in \mathbb{N}$. Montrer que si $a \mid b$ et $b \mid c$, alors $a \mid c$.

Exercice 2 Soit $n \in \mathbb{N}$ un entier non premier. Montrer que n admet un diviseur d tel que $d \leq \sqrt{n}$.

Exercice 3 Déterminer les entiers $n \in \mathbb{N}$ tels que $3^{n-1} + 5^{n-1}$ divise $3^n + 5^n$.

Exercice 4 ★ Soit $n \geq 2$, dont on note $1 = d_1 < d_2 < \ldots < d_\ell = n$ les diviseurs. On considère $m = d_1 d_2 + \cdots + d_{\ell-1} d_\ell$. Montrer que $m < n^2$, puis déterminer pour quels n est-ce que $m \mid n^2$. **Indication** : *Utiliser* $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$.

Théorème Tout entier $n \geq 2$ se décompose, de manière unique, comme produit de facteurs premiers : $n = p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}$.

Exercice 5 Soit p un nombre premier. Montrer que $\sqrt{p}$ est irrationnel. En général, pour quels entiers $n \in \mathbb{N}$ est-ce que $\sqrt{n} \in \mathbb{Q}$?

Relation de divisibilité

Propriété Soient $n, m \geq 1$ deux entiers. On note $p_1, \ldots, p_\ell$ l'ensemble des nombres premiers divisant n ou m. On écrit

$$n = p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell} \quad \text{et} \quad m = p_1^{\beta_1} \ldots p_\ell^{\beta_\ell}, \quad \text{où} \quad \alpha_i, \beta_i \geq 0.$$

Alors $n \mid m$ si et seulement si ...

Exercice 6 Avec les notations précédentes, comment se factorisent $\operatorname{pgcd}(n, m)$ et $\operatorname{ppcm}(n, m)$? Que dire de leur produit ?

Exercice 7 Soit $n \geq 1$ et ℓ le nombre de ses diviseurs premiers. Montrer que $\ln n \geq \ell \ln 2$.

Exercice 8 Soit $n = p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}$.

1. Quel est le nombre $d(n)$ de diviseurs de n ?
2. Discuter de la parité de $d(n)$.

Exercice 9 Que vaut le produit de tous les diviseurs de n ?

Exercice 10 Soient $a, b \in \mathbb{N}^*$ vérifiant $a \mid b^2$, $b^2 \mid a^3$, $a^3 \mid b^4$, etc. Autrement dit, $\forall k \in \mathbb{N}^*$, $a^{2k-1} \mid b^{2k}$ et $b^{2k} \mid a^{2k+1}$. Mq $a = b$.

Exercice 11 Soient $a, b, c \in \mathbb{N}^*$. Montrer que $\operatorname{ppcm}(a, b, c)^2 \mid \operatorname{ppcm}(a, b) \operatorname{ppcm}(b, c) \operatorname{ppcm}(c, a)$.

Divisibilité et additivité

Propriété Si $n \mid a$ et $n \mid b$, alors $n \mid a + b$, $n \mid a - b$, et $n \mid ac$, pour tout $c \in \mathbb{N}$.

Définition On dit que n et m sont premiers entre eux si leur seul diviseur commun est 1.

Exercice 12 Montrer que pour tout $n \in \mathbb{N}$, n et $2n + 1$ sont premiers entre eux. Que dire de $\operatorname{pgcd}(n, n + 2)$?

Exercice 13 Pour $n \in \mathbb{N}$, montrer que la fraction $\frac{21n+4}{14n+3}$ est irréductible.

Exercice 14

1. Montrer qu'il existe une infinité de nombres premiers.
2. Montrer qu'il existe une infinité de nombres premiers de la forme $4k - 1$.
   Ind : *Le produit de deux entiers de la forme* $4k + 1$ *est également de la forme* $4k + 1$.

Remarque Il est plus dur de montrer qu'il existe une infinité de nombres premiers de la forme $4k + 1$. On peut le déduire du fait (non trivial) qu'un entier de la forme $n^2 + 1$ ne peut pas avoir de diviseurs premiers de la forme $4k + 3$.

Exercice 15 On pose, pour $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$.

1. Factoriser $F_n - 2$ et en déduire que F_n et F_{n-1} sont premiers entre eux.
2. Montrer que tous les F_k sont deux à deux premiers entre eux, et en déduire qu'il existe une infinité de nombres premiers.

Exercice 16 Pour $n \geq 1$, on définit $a_n = 100 + n^2$ et $d_n = \operatorname{pgcd}(a_n, a_{n+1})$. Montrer que la suite (d_n) ne prend qu'un nombre fini de valeurs. *On admettra le lemme de Gauss : si $a \mid bc$ et a et b sont premiers entre eux, alors $a \mid c$.*

Exercice 17 Soit $A = \{2^n 3^{n+1},\ n \in \mathbb{N}\}$. Montrer qu'aucune somme d'éléments distincts de A n'est une puissance parfaite (c'est-à-dire s'écrire comme m^α, pour $\alpha \geq 2$).

Algèbre

Exercice 18

1. Factoriser le polynôme $x^3 - 1$, par $x - 1$. Puis factoriser $x^3 - y^3$.
2. Pour $n \in \mathbb{N}$ quelconque, factoriser $x^n - 1$ et en déduire une factorisation de $x^n - y^n$.
3. En déduire, pour n impair, une factorisation de $x^n + 1$.

Exercice 19 Montrer que si $2^n - 1$ est premier, alors n est premier.

Exercice 20 Montrer que $\operatorname{pgcd}(a^m + \cdots + 1, a - 1) = \operatorname{pgcd}(m + 1, a - 1)$.

Exercice 21 Montrer que $a^4 + 4$ n'est pas premier. **Indication** : *Chercher à factoriser cette expression, en complétant un carré.*

Équations diophantiennes

Exercice 22 ~~Montrer que les solutions de l'équation diophantienne $x^2 + y^2 = z^2$.~~

Propriété Si a et b sont premiers entre eux et ab est une puissance α-ième, alors a et b sont des puissances α-ièmes.

Exercice 23 Trouver les entiers n tels que $n(n+2)$ soit une puissance de 2.

Exercice 24

1. On considère l'équation $3^m - 2^n = 1$, d'inconnues $n, m \in \mathbb{N}$.
   - **a)** Montrer si (n, m) est solution, et $n \geq 2$, alors m est pair.
   - **b)** Trouver toutes les solutions.
2. On considère l'équation $2^n - 3^m = 1$, d'inconnues $n, m \in \mathbb{N}$.
   - **a)** Déterminer les solutions pour lesquelles m est impair.
   - **b)** En travaillant modulo 4, déterminer toutes les solutions.

Exercice 25 Trouver les entiers positifs tels que $n2^n + 1$ soit un carré.

Congruences, et applications combinatoires

On note $a \equiv b[n]$ si $n \mid a - b$. En particulier, si la division euclidienne de a par n s'écrit $a = qn + r$, on a $a \equiv r[n]$.

Propriété Si $a \equiv a'[n]$, et $b \equiv b'[n]$, alors $a + b \equiv a' + b'[n]$, $a - b \equiv a' - b'[n]$ et $ab \equiv a'b'[n]$.

Exemple Un entier n est impair ssi $n \equiv 1[2]$. Si n_1, n_2 sont deux entiers impairs, alors $n_1 n_2 \equiv 1 \times 1 \equiv 1[2]$, donc $n_1 n_2$ est impair.

Exercice 26 Calculer 9^n, puis 7^n modulo 8.

Exercice 27

1. Si x est un carré parfait, vérifier que x est forcément congru soit à 0, soit à 1 modulo 4.
2. Montrer que 2023 ne peut pas s'écrire comme la somme de deux carrés d'entiers.

Exercice 28 Montrer que parmi $n+1$ entiers $x_1, \ldots, x_{n+1}$, on peut en trouver deux dont la différence est divisible par n.

Exercice 29 On note $s(n)$ la somme des chiffres décimaux d'un entier $n \in \mathbb{N}$. Montrer que $s(n) \equiv n[9]$.

Exercice 30 ★ Calculer $s(s(s(4444^{4444})))$.

Inversibilité modulo p

Propriété – Lemme de Gauss. Soit p un nombre premier et $a, b \in \mathbb{Z}$. Si $ab \equiv 0[p]$, alors $a \equiv 0[p]$ ou $b \equiv 0[p]$.

Exercice 31 Cette propriété est-elle encore vrai pour un entier quelconque n comme modulo ? La justifier, pour p premier.

Exercice 32 Soit p un nombre premier, et $a \in [\![1, p-1]\!]$. On considère la fonction $f_a : [\![0, n-1]\!] \to [\![0, n-1]\!]$ qui à un entier x associe le reste de la division euclidienne de ax par p.

1. Montrer que f est injective, c'est-à-dire que si $x_1, x_2 \in [\![0, n-1]\!]$ vérifient $f_a(x_1) = f_a(x_2)$, alors $x_1 = x_2$.
2. En déduire qu'il existe un élément $b \in [\![1, p-1]\!]$ tel que $f_a(b) = 1$, c'est-à-dire $ab \equiv 1[p]$.
   On dit que b est un inverse de a modulo p.

Exercice 33 Théorème de Fermat Soit p premier et $a \in [\![1, p-1]\!]$. En utilisant l'application f_a précédente, et en considérant le produit $(p-1)! = 1 \times 2 \times \cdots \times (p-1)$ modulo p, montrer que $a^{p-1} \equiv 1[p]$.

Exercice 34 Théorème de Wilson Soit p premier.

1. Quels sont les éléments $x \in [\![1, p-1]\!]$ qui sont l'inverse d'eux-mêmes modulo p ?
2. En déduire que $(p-1)! \equiv -1[p]$.

Un ancien exercice du CG

Exercice 35 Soient $a, b \in \mathbb{N}$ des entiers premiers entre eux. Les résultats de l'exercice 32 restent valables en remplaçant l'hypothèse p premier par le fait que a et b soient premiers entre eux. Montrer alors que tout entier $n \geq ab$ peut s'écrire comme $au + bv$, pour $u, v \in \mathbb{N}$.

Exercice 36 On considère une suite finie à n termes $U = (u_1, \ldots, u_n)$. On dit qu'un entier strictement positif p est une période de U si l'on a $u_i = u_{i+p}$ pour tout entier i tel que $1 \leq i \leq n - p$. Une suite peut avoir plusieurs périodes.

1. On considère deux entiers strictement positifs a et b premiers entre eux.
   - **a)** On définit r_k comme le reste de la division de ka par $a + b$. Montrer que lorsque k varie dans $[\![1, a+b-1]\!]$, r_k prend toutes les valeurs de $[\![1, a+b-1]\!]$.
   - **b)** En déduire que si a et b sont périodes de U et si $n \geq a + b - 1$ alors U est constante.
2. On suppose à présent que a et b sont des entiers strictement positifs de PGCD d. Montrer que si U est périodique de périodes a et b et si $n \geq a + b - d$, alors U est de période d.
3. On considère deux entiers a et b strictement supérieurs à 1 et premiers entre eux.
   - **a)** Montrer que l'on peut partager l'intervalle $[\![1, a+b-2]\!]$ en deux sous-ensembles non vides A et B de manière que la suite V égale à 1 sur A et à 0 sur B soit de périodes a et b.
   - **b)** Le partage obtenu à la question précédente est-il unique ? Montrer que, pour tout x de A, $a + b - 1 - x$ est dans A. Quelle propriété de la suite V traduit-on ainsi ?