Chapitre 14 - TD
Arithmétique

Simon Dauguet
simon.dauguet@gmail.com

7 janvier 2025

1 Divisibilité

1.1 Divisibilité

Exercice 1 :
Montrer que $\forall n \in \mathbb{N}$,

1. $6|5n^3 + n$
2. $5|2^{2n+1} + 3^{2n+1}$
3. $9|4^n - 1 + 6n$

Exercice 2 :
Soit $n \in \mathbb{N}^*$ tel que pour tout p premier, $p|n \iff (p-1)|n$.
Montrer que $1806|n$.

Exercice 3 (Tiré de Centrale MP) :
Soit $n \in \mathbb{N}^*$. On note N le nombre de diviseur positif de n, P le produit des diviseurs positifs.
Donner une formule liant n, N et P.

Exercice 4 :
Déterminer les $n \in \mathbb{Z}$ tels que

1. $n-2|n+2$
2. $n-1|n+3$
3. $n+2|n^2+2$
4. $n-1|n^2+n+1$

Exercice 5 (Équations diophantiennes) :
Résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $12x + 9y = 22$
2. $15x + 4y = 19$
3. $7x + 13y = 11$
4. $xy = 3x + y + 2$

5. $x^2 - 6x - y^2 - 2y = 4$
6. $\frac{1}{x} + \frac{1}{y} = \frac{1}{5}$

1.2 Division euclidienne

Exercice 6 :
Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Soit q le quotient de la division euclidienne de $a-1$ par b.
Déterminer, pour tout $n \in \mathbb{N}$, le quotient de la division euclidienne de $(ab^n - 1)$ par b^{n+1}.

Exercice 7 (Développement factoriel (**)) :

1. Montrer que $\forall n \in \mathbb{N}^*$, $\exists p \in \mathbb{N}^*$, $\exists a_1, \ldots, a_p \in \mathbb{N}$ tels que $\forall k \in \{1, \ldots, p\}$, $0 \leq a_k \leq k$ et $a_p \neq 0$ tels que
$$n = \sum_{k=1}^{p} a_k k!.$$
2. Montrer que cette écriture est unique.

1.3 Congruences

Exercice 8 :
Déterminer les $n \in \mathbb{Z}$ tels que
$$10 | n^2 + (n+1)^2 + (n+3)^2$$

Exercice 9 :
Montrer que $\forall n \in \mathbb{N}$,
1. $6 | 5n^3 + n$
2. $7 | 3^{2n+2} + 2^{n+2}$
3. $11 | 3^{8n} \times 5^4 + 5^{6n} \times 7^3$
4. $9 | 4^n - 1 - 3n$

Exercice 10 :
Montrer que si n est un entier impair, alors
$$n^2 \equiv 1 \ [8]$$

Exercice 11 :
Déterminer les $a, b \in \mathbb{Z}$ tels que $3^a 7^b \equiv 1 \ [10]$.

Exercice 12 :
Montrer que $\forall n, m \in \mathbb{N}$, $3^n + 3^m + 1$ n'est jamais un carré.

2 PGCD et PPCM

Exercice 13 :
Calculer le pgcd et donner un couple pour la relation de Bézout pour les entiers a et b suivant :

1. $(a, b) = (33, 24)$
2. $(a, b) = (37, 27)$
3. $(a, b) = (270, 105)$

Exercice 14 (Équivalence de Bézout) :
Soit $a, b \in \mathbb{Z}^*$ et $d \in \mathbb{Z}$.

1. Montrer
$$\exists u, v \in \mathbb{Z},\ au + bv = d \iff (a \wedge b) | d$$
2. On suppose $d = a \wedge b$. On va résoudre l'équation $au + bv = d$ d'inconnus $u, v \in \mathbb{Z}$.
   (a) Justifier qu'il existe une solution (u_0, v_0).
   (b) Déterminer l'ensemble des couples $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = d$ à partie de (u_0, v_0).

Exercice 15 :
Soit $n \in \mathbb{N}$. Montrer que le pgcd de $2n + 4$ et $3n + 3$ ne peut être que $1, 2, 3$ ou 6.

Exercice 16 :
Soit $a, b, \lambda \in \mathbb{Z}$ et $m \in \mathbb{N}^*$. On suppose λ et m premiers entre eux. Montrer
$$a \equiv b\ [m] \iff \lambda a \equiv \lambda b\ [m]$$

Exercice 17 :
Soit $a, b, k \in \mathbb{Z}$. Montrer
$$a \wedge b = (a + kb) \wedge b$$

Exercice 18 :
Résoudre dans $\mathbb{N}^2$ les systèmes

1. $\begin{cases} \text{pgcd}(x, y) = 5 \\ \text{ppcm}(x, y) = 60 \end{cases}$
2. $\begin{cases} x + y = 100 \\ \text{pgcd}(x, y) = 10 \end{cases}$

Exercice 19 :
Soit $d, m \in \mathbb{N}$. Donner une condition nécessaire et suffisante sur d et m pour que le système
$$\begin{cases} x \wedge y = d \\ x \vee y = m \end{cases}$$
admette au moins une solution $(x, y) \in \mathbb{N}^2$.

Exercice 20 (**) :
Soit $a, b \in \mathbb{N}$ et $b \neq 0$.

1. Montrer que si r est le reste de la division euclidienne de a par b, alors $2^r - 1$ et le reste de la division euclidienne de $2^a - 1$ par $2^b - 1$.

2. En déduire
$$(2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1.$$

Exercice 21 :
Soit $a, b, c \in \mathbb{Z}$ avec $a \wedge c = 1$.

1. Montrer que $a \wedge (bc) = a \wedge b$
2. Que dire de $a \vee (bc)$?

Exercice 22 (**) :
Soit $a, b \in \mathbb{Z}$ premiers entre eux et $d \in \mathbb{N}^*$ tel que $d|ab$. Montrer
$$\exists!(d_1, d_2) \in \mathbb{N}^2,\ d_1|a,\ d_2|b,\ d = d_1 d_2.$$

Exercice 23 :
Résoudre dans $\mathbb{N}^*$ l'équation $x \wedge y + x \vee y = y + 4$.

Exercice 24 :
Soit $a, b \in \mathbb{Z}$. Calculer $(a + b) \wedge (a \vee b)$.

Exercice 25 (**) :
Soit $a, b \in \mathbb{Z}$ premiers entre eux. Montrer que
$$\varphi : \begin{array}{ccc} \mathrm{Div}_+(a) \times \mathrm{Div}_+(b) & \to & \mathrm{Div}_+(ab) \\ (d, d') & \mapsto & dd' \end{array}$$
est bijective.

3 Les nombres premiers

3.1 Primalité

Exercice 26 (nombres composés) :
Montrer que les nombres suivants ne sont pas premiers :

1. $4n^3 + 6n^2 + 4n + 1$ avec $n \in \mathbb{N}^*$
2. $n^4 - n^2 + 16$ avec $n \in \mathbb{Z}$.

Exercice 27 :
Soit $n \geq 2$ et N la somme de n entiers impairs consécutifs. Montrer que N n'est pas un nombre premier.

Exercice 28 (Intervalle contenant un nombre premier) :
Soit $n \in \mathbb{N}^*$. Montrer qu'il existe toujours un nombre premier strictement compris entre n et $n! + 2$.

Exercice 29 (Nombres de Fermat (**)) :

1. [Centrale MP] Montrer que si $n \geq 2$ tel que $2^n - 1$ est premier, alors n est premier.
2. Soit $a, p \geq 2$. Montrer que si $a^p - 1$ est premier, alors $a = 2$ et p est premier.
3. [Mines MP] Soit $a \geq 2$ et $n \geq 1$. Montrer que si $a^n + 1$ est premier, alors n est une puissance de 2.

Remarque :
Fermat a conjecturé que tous les $F_n = 2^{2^n} + 1$ sont premiers. C'est faux pour $n \in \{5, \ldots, 32\}$. On ne sait rien dire, pour le moment, pour les nombres F_n avec $n \geq 33$.

3.2 Valuations p-adiques, Fermat etc

Exercice 30 :
Soit $a, b \in \mathbb{Z}$. Montrer

$$a|b \iff a^2|b^2$$

Exercice 31 (Irrationalité [✓]) :
On considère l'équation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

d'inconnue x et où $a_0, \ldots, a_{n-1} \in \mathbb{N}$.

Montrer que les solutions réelles de cette équation sont soient entières soient irrationnelles.

Exercice 32 :
Montrer que pour tout nombre premier p, $p^4 + 4$ n'est pas premier. On le fera par deux méthodes différentes.

Exercice 33 (Théorème RSA (*) [✓]) :
Soit $p, q \in \mathcal{P}$, $p \neq q$. On pose $n = pq$ et $e \in \mathbb{N}$ premier avec $(p-1)(q-1)$.

1. Justifier $\exists d \in \mathbb{N}$ tel que $ed \equiv 1\ [(p-1)(q-1)]$.
2. Montrer que $\forall x \in \mathbb{N}$, $x^{ed} \equiv x\ [n]$.

Remarque :
Ce théorème est la base de la cryptologie informatique. e est la clé publique connus de tous. x est l'information à coder. x^e est le message codé. Pour le décoder, il faut connaître d, la clé privée, qui permet de retrouver x.

Exercice 34 (Infinité de premier de la forme $4n+1$ (**)) :
On veut montrer qu'il existe une infinité de nombres premiers de la forme $4n+1$. On raisonne par l'absurde. On suppose donc qu'il y en a un nombre fini. Soit N le produit de ces nombres premiers. On pose $M = 4N^2 + 1$.

1. Supposons qu'il existe un nombre premier $q \equiv 3\ [4]$ tel que $q|M$. Montrer que

$$(2N)^{q-1} \equiv -1\ [q].$$

2. Conclure en utilisant le petit théorème de Fermat.

Exercice 35 (Triplets pythagoriciens (***)) :
Le but de cet exercice est de montrer une partie du dernier théorème de Fermat : on va résoudre l'équation $x^2 + y^2 = z^2$ dans $\mathbb{N}^*$.

1. Trouver une solution à cette équation, puis généraliser pour montrer qu'il existe une infinité de solutions.

2. Soit $(x, y, z) \in (\mathbb{N}^*)^3$. Montrer que

$$x^2 + y^2 = z^2 \iff \exists x', y', z', n \in \mathbb{N}^*,\ x' \wedge y' \wedge z' = 1,\ x'^2 + y'^2 = z'^2,\ x = nx',\ y = ny',\ z = nz'.$$

3. Soit $x, y, z \in \mathbb{N}^*$ tels que $x^2 + y^2 = z^2$. On suppose x, y et z premiers dans leur ensemble.
   (a) Montrer que x et y ne sont pas de même parité.
   (b) On suppose x pair et y impair. On pose $x = 2u$, $z - y = 2v$ et $z + y = 2w$. Montrer que v et w sont premiers entre eux.
   (c) Montrer qu'il existe $m, n \in \mathbb{N}$ de parité différentes tels que $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$.
4. Étudier la réciproque et résoudre l'équation $x^2 + y^2 = z^2$.

Remarque :
Un triplet $(a, b, c) \in \mathbb{N}^3$ tels que $a^2 + b^2 = c^2$ s'appelle un triplet pythagoricien. Ce sont les côtés d'un triangle rectangle.