

LICENCE. ARITHMÉTIQUE ET ALGÈBRE. 2010/2011. Version 0.

VERSION TRÈS PROVISoire. LES CHAPITRES AVEC * NE SONT PAS AU PROGRAMME DU PARTIEL D'OCTOBRE 2010.

Table des matières

1	ENTIERS, DIVISIBILITÉ, CONGRUENCES.	3
1.1	Division eulidienne.	3
1.2	Exercices.	3
1.3	Idéaux de \mathbb{Z}	5
1.4	Pgcd, ppcm.	6
1.5	Théorème de Bezout.	6
1.6	Algorithme d'Euclide.	8
1.7	Exercices	8
2	DÉCOMPOSITION EN FACTEURS PREMIERS.	11
2.1	Décomposition en facteurs premiers.	11
2.2	Exercices	13
2.3	*Décomposition en facteurs premiers de $n!$	16
2.4	Exercices	18
3	CONGRUENCES.	20
3.1	Congruences modulo n , Opérations.	20
3.2	exercices	22
3.3	Le 'petit' théorème de Fermat. Applications à la factorisation.	24
3.4	Exercices.	27
3.5	*Nombres pseudopremiers.	28
3.6	Exercices	29
3.7	*Théorème d'Euler. Symbole de Legendre.	30
3.8	Exercices.	31
3.9	*Théorème de Wilson.	32
3.10	Exercices	32
4	ÉLÉMENTS INVERSIBLES DE \mathbb{Z}_n^*.	33
4.1	Éléments inversibles de \mathbb{Z}_n	33
4.2	exercices	33
4.3	Théorème Chinois.	34
4.4	Exercices.	35
4.5	Indicatrice d'Euler.	35
4.6	Exercices.	36
4.7	*Fonctions multiplicatives.	39
4.8	Exercices.	39
4.9	Généralisation d'Euler du petit théorème de Fermat.	40

4.10	*Ordre multiplicatif d'un élément de \mathbb{Z}_n^*	41
4.11	Exercices.	42
5	Sujet du partiel d'octobre 2009.	45

1 ENTIERS, DIVISIBILITÉ, CONGRUENCES.

1.1 Division euclidienne.

Soit \mathbb{Z} l'ensemble des entiers naturels (positifs ou négatifs). Il est muni de deux opérations l'addition $+$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ et la multiplication \times : $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ qui en font un **anneau**¹ commutatif. On note $a.b = a \times b$ le produit de $a \in \mathbb{Z}$ et de $b \in \mathbb{Z}$.

On a, en particulier : $a.(b + c) = a.b + a.c$, pour tous $a, b, c \in \mathbb{Z}$.

Pour tout nombre réel $x \in \mathbb{R}$, on note $[x] \in \mathbb{Z}$ sa 'partie entière', définie comme l'unique entier m tel que $m \leq x < m + 1$. On a donc une écriture unique : $x = [x] + \{x\}$, avec $\{x\} := x - [x]$, la 'partie fractionnaire' de x , telle que : $0 \leq \{x\} < 1$.

Division Euclidienne : Rappelons que si $a, b > 0$ sont des entiers (de \mathbb{Z}), il existe un unique couple (q, r) (dépendant de (a, b)) d'entiers tels que :

1. $a = b.q + r$
2. $0 \leq r < b$.

On appelle q (resp. r) le **quotient** (resp. le **reste**) de la division euclidienne de a par b .

Explicitement : $q = [\frac{a}{b}]$, $r = a - [\frac{a}{b}].b$ (en notant $[x]$ la partie entière du réel x).

Démonstration : Existence : $a = [\frac{a}{b}].b + (a - [\frac{a}{b}].b)$, et on vérifie que le couple $(q := [\frac{a}{b}], r := a - [\frac{a}{b}].b)$ satisfait les conditions imposées.

Unicité : si l'on a deux telles expressions : $a = q.b + r = q'.b + r'$, on peut supposer que $q \geq q'$, donc $b > r' - r = (q - q').b \geq 0$. On a donc $1 > q - q' \geq 0$, donc $q = q'$ et enfin $r = r'$. \square

Divisibilité : Soit a, b des entiers. On dit que b **divise** a (ou que a est un **multiple** de b) s'il existe $c \in \mathbb{Z}$ tel que : $a = b.c$. Ceci équivaut donc au fait que le reste de la division euclidienne de a par b est nul, ou encore au fait que $a.\mathbb{Z} \subset b.\mathbb{Z}$, en notant $a.\mathbb{Z} := \{a.k, k \in \mathbb{Z}\}$ l'ensemble des multiples de a . Par exemple, tout $a \in \mathbb{Z}$ divise 0.

1.2 Exercices.

Exercice 1.1 Si $a, b \in \mathbb{R}$, montrer que $[a] + [b] \leq [a + b] \leq [a] + [b] + 2$. Cet encadrement est-il optimal ?

Quel encadrement similaire optimal peut-on donner de $[a_1 + \dots + a_n]$ si les a_j sont n nombres réels ?

Exercice 1.2 Montrer, si $x \in \mathbb{R}$, que : $-[-x] = [x]$ si $x \in \mathbb{Z}$, et que : $-[-x] = [x] + 1$ sinon.

¹La définition est donnée en ??

Exercice 1.3 Si $x, y \in \mathbb{R}$, montrer que $[2x] + [2y] \geq [x] + [x + y] + [y]$. (Se ramener au cas où : $0 \leq x \leq y < 1$).

Exercice 1.4 Montrer que $\sum_{k=0}^{n-1} [x + \frac{k}{n}] = [nx]$. (Se ramener au cas où : $0 \leq x < 1$).

Exercice 1.5 Si n, d, d' sont des entiers strictement positifs arbitraires, montrer que : $[\frac{n}{d.d'}] = [\frac{[\frac{n}{d}]}{d'}]$. En déduire que pour tout $x = \frac{u}{v} \in \mathbb{Q}$, et pour tout entier $d > 0$, on a : $[\frac{x}{d}] = [\frac{[x]}{d}]$, et que $\{\frac{x}{d}\} = \{\frac{[x]}{d}\} + \frac{\{x\}}{d}$.

Exercice 1.6 Si n, m sont des entiers strictement positifs arbitraires, montrer que : $[\frac{n+1}{m}] = [\frac{n}{m}]$ si m ne divise pas $(n + 1)$, et que : $[\frac{n+1}{m}] = [\frac{n}{m}] + 1$ si m divise $(n + 1)$.

Exercice 1.7 Déterminer le reste et le quotient de la division de $n^2 + 3n + 1$ par $n - 1$. (Remplacer n par $(n - 1) + 1$).

Exercice 1.8 Si a_1, \dots, a_n, \dots sont des entiers tous au moins égaux à 2, alors tout entier positif n s'écrit de manière unique sous la forme :

$$n = t_0 + t_1.a_1 + t_2.a_1.a_2 + \dots + t_d.a_1 \dots a_d, \text{ avec des entiers } 0 \leq t_j < a_{j+1}.$$

Exercice 1.9 Soit $a, b, m \in \mathbb{Z}$. On suppose que m divise a et b .

0. Montrer que, pour tous $u, v \in \mathbb{Z}$, m divise $au + bv$.

On pose : $d = 0$ si $a = b = 0$. Sinon, soit d le plus petit des entiers $n > 0$ de la forme : $au + bv, u, v \in \mathbb{Z}$.

1. Déterminer d si $a = 0, b \neq 0$.

On suppose désormais que $a.b \neq 0$. Montrer que :

2. $d > 0$, et que m divise d . (Ecrire $a = a'.m$ et $b = b'.m$).

3. d divise a et b . (Remarquer que le reste r de la division de a par e est de la forme $au' + bv'$, et que $0 \leq r < d$. Procéder de même pour b).

4. d est aussi le plus grand des entiers $n > 0$ qui divisent a et b . On l'appelle le **plus grand commun diviseur** de a et b , noté $\text{pgcd}(a, b)$, ou simplement : (a, b) .

5. un entier $n \in \mathbb{Z}$ divise a et b si et seulement si n divise d .

6. un entier $n \in \mathbb{Z}$ est de la forme $au + bv$ si et seulement si d divise n .

Exercice 1.10 Montrer que $(a, b - ua) = (a, b)$, pour tout $u \in \mathbb{Z}$, et que $(a, b) = (a, r)$ si r est le reste de la division euclidienne de a par b . En déduire une méthode de calcul de (a, b) par divisions successives, et un couple $u, v \in \mathbb{Z}$ tel que $(a, b) = au + bv$. ("Algorithme d'Euclide").

Exercice 1.11 Montrer que, pour tous $k \in \mathbb{Z}$, on a : $(a.k, b.k) = (a, b).k$.

Montrer que $(a', b') = 1$ si $a' := a/d$ et si $b' = b/d$, en posant : $d = (a, b)$.

1.3 Idéaux de \mathbb{Z} .

Definition 1.12 Un idéal² de \mathbb{Z} est un sous-ensemble $J \subset \mathbb{Z}$ tel que :

1. $0 \in J$
2. $x - y \in J$ si $x, y \in J$

Remarque 1.13 Si J est un idéal de \mathbb{Z} , et si $x, y \in J$, $k \in \mathbb{Z}$, alors :

1. $-y \in J$.
2. $x + y \in J$.
3. $k.x \in J$. (Faire une récurrence sur k si $k \geq 0$, puis utiliser l'égalité : $(-k).x = -k.x$ sinon).

Exemple 1.14 1. Si $b \in \mathbb{Z}$, on note $b.\mathbb{Z}$ l'ensemble de tous les multiples $b.c$, $c \in \mathbb{Z}$ de b . C'est un idéal de \mathbb{Z} . On a : $b.\mathbb{Z} = \{0\}$ (resp. $b.\mathbb{Z} = \mathbb{Z}$) si et seulement si $b = 0$ (resp. $b = +1$ ou $b = -1$).

2. $a.\mathbb{Z} \subset b.\mathbb{Z}$ si et seulement si : b divise a .

3. Si J, K sont des idéaux de \mathbb{Z} , on peut définir deux nouveaux idéaux de \mathbb{Z} : leur **intersection** $J \cap K$ et leur **somme** $J + K := \{u + v, \text{ où } : u \in J, v \in K\}$. Donc : $J + K$ est le plus petit idéal de \mathbb{Z} contenant J et K , tandis que $J \cap K$ est le plus grand idéal de \mathbb{Z} contenu dans J et dans K .

4. Par exemple, si $a, b \in \mathbb{Z}$, alors : $a.\mathbb{Z} + b.\mathbb{Z} = \{a.x + b.y, \text{ où } x, y \in \mathbb{Z} \text{ sont arbitraires}\}$.

Théorème 1.15 Tout idéal J de \mathbb{Z} est **principal** (c'est-à-dire qu'il existe $b \in \mathbb{Z}$ tel que : $J = b.\mathbb{Z}$). On dit que b est un **générateur** de J .

Démonstration : Si $J = \{0\}$, on prend $b = 0$. Sinon, il existe $0 \neq w \in J$. On peut supposer $w > 0$ (sinon $0 < -w \in J$). Soit alors $b > 0$ le plus petit élément strictement positif de J (qui existe car c'est le plus petit élément de $\{1, 2, \dots, w\} \cap J$). On va montrer que $J = b.\mathbb{Z}$.

On a $b.\mathbb{Z} \subset J$, puisque $b \in J$.

Soit $a \in J$. On va montrer que a est un multiple de b , ce qui achèvera la démonstration. On divise a par b : $a = b.q + r$. On a : $a, b \in J$. Donc $b.q \in J$, donc $a - b.q = r \in J$. Mais $0 \leq r < b$. Donc $r = 0$, et $a = b.q$ \square

Remarque 1.16 Si $J = \{0\}$, J a un seul générateur : $b = 0$. Sinon, J a deux générateurs, dont un seul est strictement positif. C'est toujours celui-ci que nous choisirons.

²Ce sont aussi, plus simplement, les sous-groupes de $(\mathbb{Z}, +)$.

1.4 Pgcd, ppcm.

Definition 1.17 Soit $(a, b) \in \mathbb{Z}$ on appelle $d := \text{pgcd}(a, b) := (a, b)$ (resp. $m := \text{ppcm}(a, b) := (a \cap b)$) le générateur positif ou nul de l'idéal $a.\mathbb{Z} + b.\mathbb{Z}$ (resp. $a.\mathbb{Z} \cap b.\mathbb{Z}$).

Proposition 1.18 Pour a, b, d, m comme ci-dessus :

1. d est le “plus grand commun diviseur” de a et b : $c \in \mathbb{Z}$ divise a et b si et seulement s'il divise d .

2. m est le “plus petit commun multiple” de a et b : $c \in \mathbb{Z}$ est multiple de a et de b si et seulement s'il est multiple de m .

Démonstration : Par hypothèse, il existe $x, y \in \mathbb{Z}$ tels que $d = a.x + b.y$ Si c divise a et b il divise donc $a.x + b.y = d$.

Réciproquement, si c divise d , il divise a et b , puisque d les divise, car $a, b \in d.\mathbb{Z}$.

Pour le ppcm : démonstration analogue \square

Remarque 1.19 1. (a, b) (resp. $a \cap b$) est donc aussi le plus petit élément positif ou nul de l'ensemble des nombres de la forme $a.x + b.y, x, y \in \mathbb{Z}$ (resp. simultanément de la forme $a.x$ et $b.y$).

2. $(a, b) = (a - k.b, b)$, pour tout $k \in \mathbb{Z}$, puisque $a.\mathbb{Z} + b.\mathbb{Z} = (a - k.b).\mathbb{Z} + b.\mathbb{Z}$. En effet : $(a - k.b).x + b.y = a.x + b.(y - k.x)$. Cette remarque est à la base de l'algorithme d'Euclide, exposé ci-dessous.

3. On peut définir aussi le pgcd et le ppcm d'un ensemble fini d'entiers (a_1, \dots, a_m) , comme étant le générateur positif de l'idéal $a_1.\mathbb{Z} + \dots + a_m.\mathbb{Z}$ (resp. $a_1.\mathbb{Z} \cap \dots \cap a_m.\mathbb{Z}$).

Ces nombres se calculent par récurrence sur $m \geq 3$: $\text{pgcd}(a_1, \dots, a_m) = \text{pgcd}(a_1, \text{pgcd}(a_2, \dots, a_m))$ et $\text{ppcm}(a_1, \dots, a_m) = \text{ppcm}(a_1, \text{pppcm}(a_2, \dots, a_m))$.

Proposition 1.20 Soit $a, b, k \in \mathbb{Z}$. Alors :

0. (a', b') divise (a, b) si a' divise a et si b' divise b .

1. $(ak, bk) = (a, b).k$

2. $ak \cap bk = (a \cap b).k$.

3. $(a', b') = 1$ si $a' := a/d$ et $b' := b/d$, avec $d := (a, b)$.

Démonstration :

0. $(a, b).\mathbb{Z} = a.\mathbb{Z} + b.\mathbb{Z} \subset (a'.\mathbb{Z} + b'.\mathbb{Z}) = (a', b').\mathbb{Z}$, puisque $a.\mathbb{Z} \subset a'.\mathbb{Z}$ et $b.\mathbb{Z} \subset b'.\mathbb{Z}$.

1. $ak.\mathbb{Z} + bk.\mathbb{Z} = k.(a.\mathbb{Z} + b.\mathbb{Z})$. D'où 3.

2. $ak.\mathbb{Z} \cap bk.\mathbb{Z} = k.(a.\mathbb{Z} \cap b.\mathbb{Z}) \square$

1.5 Théorème de Bezout.

Definition 1.21 Soit $a, b \in \mathbb{Z}$. On dit que a, b sont premiers entre eux si $(a, b) = \text{pgcd}(a, b) = 1$.

On déduit de la définition 1.17 le :

Théorème (de Bezout) : *a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$.*

Exemple 1.22 *Pour tous $k, n \in \mathbb{Z}$, n et $k.n + 1$ sont premiers entre eux.*

Proposition 1.23 *Soit $a, b, c \in \mathbb{Z}$, tels que $(a, b) = 1$. On a les propriétés suivantes :*

1. *si $b \mid a.c$, alors : $b \mid c$ (Lemme d'Euclide).*
2. *si $a \mid c$, et si $b \mid c$, alors : $ab \mid c$.*
3. *$(a \cap b) = \mid ab \mid$*
4. *si $(a, c) = 1$, alors : $(a, bc) = 1$.*
5. *$(a^m, b^n) = 1, \forall m, n$ entiers positifs.*

Démonstration : On fixe $u, v \in \mathbb{Z}$ tels que $a.u + b.v = 1$

1. Si $a.c = k.b$, donc $k.b.u + b.c.v = a.c.u + b.c.v = c$, et $b.(ku + cv) = c$.
2. Si $c = ka = k'b$, alors : $c = acu + bcv = ak'bu + bkav = ab.(k'u + kv)$.
3. La propriété 2 montre que $a.b$ divise $a \cap b$. Puisque $a \cap b$ divise toujours ab , on a l'égalité.

4. Si $as + ct = 1$, alors : $(as + ct).(au + bv) = 1 = a.(asu + sbv + uct) + bc.tv$.
Donc $(a, bc) = 1$.

5. $(a, b^m) = 1$ par récurrence sur $m \geq 1$, à l'aide de 3. Ensuite, appliquer ce qui vient d'être établi au couple $(b^m, a) \square$

Corollaire 1.24 *Si $a, b \in \mathbb{Z}$, on a : $(a \cap b).(a, b) = \mid ab \mid, \forall a, b \in \mathbb{Z}$.*

Démonstration : On pose : $d := (a \cap b)$, $a' := a/d, b' := b/d$. Alors $d = (a'.d, b'.d) = d.(a', b')$. Donc : $(a', b') = 1$ et $(a' \cap b') = a'.b'$, par 1.23.3 ci-dessus. Puisque $a \cap b = a'.d \cap b'.d = d.(a' \cap b') = d.a'.b' = (a.b)/d$, on a : $d.(a \cap b) = a.b \square$

Remarque 1.25 *L'hypothèse de primalité relative ci-dessus est essentielle.*

Par exemple, supposons $a = b > 1$.

Pour 1 : Si $c = 1$, $b = a$ divise $a.c = a.1 = a$, mais ne divise pas $c = 1$.

Pour 2 : si $c = a$, alors a et $b = a$ divisent $c = a$, mais $ab = a^2$ ne divise pas a .

Proposition 1.26 *Soit $n, ab, c \in \mathbb{Z}$. Si n divise $a.b$, et si $(a, b) = 1$, alors $n = a'.b'$, où : $a' := (n, a)$ et $b' := (n, b)$.*

Démonstration : On a : $(a', b') = (a', b) = (a, b') = (a, b) = 1$, puisque les trois premiers termes divisent le dernier. Donc $a' \cap b' = a'.b'$ divise n , et aussi $a.b$. Puisque $n/a'.b'$ divise $a.b/a'.b' = (a/a').(b/b')$, et que $n/a'.b'$, qui divise n/a' et n/b' est donc premier avec a/a' et b/b' , il divise b/b' et a/a' , donc leur *pgcd*, qui est égal à 1. Donc $n/a'.b' = 1 \square$

1.6 Algorithme d'Euclide.

Il permet, par divisions successives, de calculer $d := (a, b)$, et trouver $u, v \in \mathbb{Z}$ tels que $d = a.u + b.v$.

On part de $0 < a < b \in \mathbb{Z}$ (car $(a, b) = (-a, b) = (a, -b) = (-a, -b) = (b, a)$).

On effectue la division euclidienne de b par a : $b = aq + r$. Deux cas : ou bien $r = 0$, $(a, b) = a$ on a fini. Ou bien $a > r > 0$, alors $(a, b) = (r, a)$. On remplace a (resp. b) par r (resp. a). On recommence. Le processus s'arrête dès que l'on obtient un reste nul. Ce qui se produit après au plus $(a - 1)$ itérations (récurrence sur a).

En fait le nombre d'itérations est, au plus, $2.\log_2(a)$, proportionnel au plus au nombre de chiffres décimaux de a .

Ce calcul fournit aussi u, v tels que $ua + vb = (a, b)$. On voit ceci par récurrence sur le nombre de divisions. En effet, si $a.u' + r.v' = d$ avec les notations ci-dessus, alors : $d = a.u' + (b - qa).v' = a.(u' - q.v') + b.v'$.

Exemple 1.27 Calculer $(59, 21)$. Trouver des solutions $u, v \in \mathbb{Z}$ de l'équation : $u.59 + v.21 = 1$.

Par divisions successives :

$$59 = 2.21 + 17$$

$$21 = 1.17 + 4$$

$$17 = 4.4 + 1$$

$$4 = 4.1 + 0$$

$$\text{Donc } (59, 21) = 1.$$

Pour résoudre l'équation $59.u + 17.v = 1$, on procède comme suit :

$$1 = 17 - 4.4 = 17 - 4.(21 - 17) = (1 + 4).17 - 4.21 = 5.17 - 4.21 = 5.(59 - 2.21) - 4.21 = 5.59 - (5.2 + 4).21 = 5.59 - 14.21. \text{ D'où la solution : } u = 5, v = -14.$$

1.7 Exercices

Exercice 1.28 Montrer (par récurrence sur $m \geq 3$) que : $\text{pgcd}(a_1, \dots, a_m) = \text{pgcd}(a_1, \text{pgcd}(a_2, \dots, a_m))$ et $\text{ppcm}(a_1, \dots, a_m) = \text{ppcm}(a_1, \text{pppcm}(a_2, \dots, a_m))$.

Exercice 1.29 Calculer les pgcd. suivants :

1. $\text{pgcd}(n - 1, n + k), k = 1, 2, 3$.
2. $\text{pgcd}(n! + 1, (n + 1)! + 1)$. Distinguer selon la parité de n .
3. $\text{pgcd}(n^2 + 1, n(n^2 - 1))$. Distinguer selon la parité de n .

Exercice 1.30 Montrer (dans \mathbb{Z}) que ab divise cd si a divise c , si b divise c , et si $d = (a, b)$.

Exercice 1.31 1. Si $n > 0$ divise $a.b$ et si $(a, b) = 1$, montrer que $n = (n, a).(n, b)$. (On montrera que (n, a) et (n, b) sont premiers entre eux, et que leur produit, noté m , divise n ; montrer enfin que $q := \frac{n}{m} = 1$, en observant que q est premier avec $\frac{a}{(n, a)}$ et $\frac{b}{(n, b)}$).

2. Montrer que si n divise $a.b$, alors $n = a'.b'.d'$, où : $d := (a, b)$, $d' := (n, d) = (n, (a, b))$, $a' := (n/d', a/d)$, $b' := (n/d', b/d)$. (Appliquer 1, en remarquant que n' divise $\frac{a.b}{d^2}$).

Exercice 1.32 Montrer que, pour tous entiers a, b, c , on a :

1. $(c, a \cap b) = (c, a) \cap (c, b)$.
2. $(a \cap b, b \cap c, c \cap a) = ((a, b) \cap (b, c) \cap (c, a))$.

Exercice 1.33 Déterminer $d := \text{pgcd}(A, B)$, avec : $A := 2^a - 1, B := 2^b + 1$ si $a, b > 1$ sont entiers, et a impair. Indication : déterminer le reste de la division par d de $2^{ab} = (A+1)^b = (B-1)^a$. Montrer sur un exemple que la condition 'a impair' ne peut être omise en conservant la conclusion obtenue.

Exercice 1.34 1. Déterminer le pgcd d de 560 et 1176 par deux méthodes.

2. Déterminer les solutions entières x, y de l'équation : $560.x + 1176.y = d$.

Exercice 1.35 Résoudre en nombres entiers (x, y) le système :

$$3x + 7y = 1, 56x + 35y = 10.$$

Exercice 1.36 Si $a > 1$ est entier, si $mn \geq 1$ sont entiers, et si $d := \text{pgcd}(m, n)$, montrer que $\text{pgcd}(M, N) = D$, si $M := a^m - 1, N := a^n - 1, D := a^d - 1$. On pourra montrer d'abord que D divise M et N , et donc leur PGCD. On montrera ensuite que si $d = u.m - v.n$, avec $u, v \in \mathbb{Z}$ positifs, alors $D = U.M - V.N$, avec U, V entiers positifs. (On pourra écrire : $N.V + D := (N.V' + 1).(D + 1) - 1 := (N + 1)^v.(D + 1) - 1 = (a^n)^v.a^d - 1 = a^{v.n+d} - 1 = a^{u.m} - 1 = (a^m)^u - 1 = (M + 1)^u - 1 := M.U$).

Exercice 1.37 Montrer que $\text{ppcm}(a^2, b^2) = \text{ppcm}(a^2, ab, b^2)$. Indication : se ramener au cas où $(a, b) = 1$ en divisant par (a, b) .

Généraliser (considérer : $\text{ppcm}(a^n, a^{n-1}.b, \dots, a^j.b^{n-j}, \dots, b^n)$).

Exercice 1.38 Montrer qu'il n'existe pas d'entiers $u > 0, v > 0$ tels que $u^2 = 2.v^2$. Indication : se ramener au cas où $d := (a, b) = 1$ en divisant par d^2 .

En déduire que si $a, b \in \mathbb{Z}$ sont tels que $a + b\sqrt{2} = 0$, alors : $a = b = 0$.

Exercice 1.39 Montrer que $\text{pgcd}(a, b) = \text{pgcd}(a + 2b, a + b)$. En déduire que, si $(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}$, alors $\text{pgcd}(a_n, b_n) = 1$. Montrer, de plus, que $a_n^2 - 2b_n^2 = (-1)^n$. En déduire que $a_n/b_n \rightarrow \sqrt{2}$.

Exercice 1.40 Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice à coefficients dans \mathbb{Z} , et si

$\begin{pmatrix} m' \\ n' \end{pmatrix} = A \begin{pmatrix} m \\ n \end{pmatrix}$ (autrement dit, $m' = am + bn, n' = cm + dn$), montrer que :

1. $\text{pgcd}(m', n')$ divise $\det(A).\text{pgcd}(m, n)$. (On pourra, par exemple, multiplier à gauche A par A^* , la transposée de sa comatrice).

2. $\text{pgcd}(m', n') = \text{pgcd}(m, n)$, si $\det(A) = ad - bc = \pm 1$.

3. il existe (m, n) tel que $(m, n) = 1$ et $\text{pgcd}(m', n') = \det(A) \cdot \text{pgcd}(m, n)$ si $\text{pgcd}(a, b, c, d) = 1$.

4. $\text{pgcd}(a, b, c, d) \cdot \text{pgcd}(m', n')$ divise $\det(A) \cdot \text{pgcd}(m, n)$, pour tout (m, n) .

5. il existe (m, n) tel que $\text{pgcd}(a, b, c, d) \cdot \text{pgcd}(m', n') = \det(A) \cdot \text{pgcd}(m, n)$ et $(m, n) = 1$.

Exercice 1.41 Si $N = a^4$ est divisible par 5, quel sont les 4 derniers chiffres de N ?

Exercice 1.42 Si a_1, \dots, a_n sont des entiers positifs, montrer que le ppcm des a_j est égal à $\prod_{j=1}^{j=k} P_j^{(-1)^{j+1}}$, où P_j est le produit des pgcd des a_k pris j à j . Procéder par récurrence sur k ou par décomposition en produit de facteurs premiers.

Exercice 1.43 Soit $a > 1$, $m > 0$ et $n > 0$ des entiers. Soit $d := (m, n)$ et $N := (a^m - 1, a^n - 1)$ les PGCD.

1. Montrer que $(a^d - 1)$ divise N . (On pourra écrire : $m = d \cdot \ell$, puis $a^m = (a^d)^\ell$, et utiliser une factorisation du polynôme $(X^\ell - 1)$).

2. Montrer que N divise $(a^r - 1)$, pour tout $r \geq 0$ de la forme $r = um + vn$, avec $u, v \in \mathbb{Z}$. (Considérer la différence : $(a^{um} - 1) - (a^{vn} - 1)$ et la factoriser par a^{vn}).

3. En déduire que $N = (a^d - 1)$.

4. Déterminer le PGCD de 999.999 et de 999.999.999 (dans le système décimal).

Exercice 1.44 Soit $a = a_0 > b = a_1 > 0$ entiers. Soit a_r la suite d'entiers définie par l'algorithme d'Euclide : $a_r = q_r \cdot a_{r+1} + a_{r+2}$.

1. Montrer que $a_r > 2 \cdot a_{r+2}$.

2. Montrer que l'algorithme termine en, au plus, s divisions, si s est le nombre de chiffres de l'écriture de a en base 2.

3. Montrer que l'algorithme termine en, au plus, $(\frac{10}{3}) \cdot t$ divisions, si t est le nombre de chiffres de l'écriture décimale de a . Indication : utiliser l'inégalité : $2^{10} = 1024 > 10^3$.

Exercice 1.45 * La suite de Fibonacci est la suite croissante d'entiers $f_k, k \geq 1$ définie par récurrence par : $f_1 = f_2 = 1$ et $f_{k+1} := f_k + f_{k-1}$ si $k \geq 3$.

1. Montrer que, pour tout k , $f_k = \frac{u^k - v^k}{\sqrt{5}}$ si $u = \frac{1+\sqrt{5}}{2}$ et $v = \frac{1-\sqrt{5}}{2}$ sont les racines de l'équation $X^2 - X - 1 = 0$.

2. En déduire que $f_k = \lfloor \frac{u^k}{2 \cdot \sqrt{5}} \rfloor$ si k est pair, et que $f_k = \lfloor \frac{u^k}{2 \cdot \sqrt{5}} \rfloor + 1$ si k est impair.

3. Montrer que $(f_k, f_{k+1}) = 1$ si $k \geq 1$, et que l'algorithme d'Euclide pour le calcul de ce pgcd nécessite $(k - 2)$ divisions euclidiennes si $k \geq 2$. Procéder par récurrence sur k .

4. Déterminer les solutions $(u, v) \in \mathbb{Z}^2$ de l'équation de Bezout $u \cdot f_k + v \cdot f_{k+1} = 1$. On pourra procéder par récurrence sur $k \geq 2$ en distinguant selon la parité de k .

5. Soit $a > b > 0$ entiers. Si l'algorithme d'Euclide pour calculer (a, b) nécessite k divisions, montrer que $a \geq f_{k+2}$.

2 DÉCOMPOSITION EN FACTEURS PREMIERS.

2.1 Décomposition en facteurs premiers.

Soit $p \geq 2$ un entier. On dit que p est **premier** si les seuls entiers $a > 0$ qui divisent p sont 1 et p . Les nombres premiers sont, par ordre croissant : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Remarque 2.1 Soit $n > 0$ un entier. Soit p le plus petit des diviseurs d de n tels que $d > 1$. Alors p est premier, puisqu'il n'a pas de diviseur $1 < d < p$. On a donc : $p = n$ si et seulement si n est premier. De plus, si n n'est pas premier, $p < n$, et donc : $p \leq \sqrt{n}$, puisque $1 < n/p$ est aussi un diviseur de n , de sorte que $n = p.(n/p) \geq p.p = p^2$.

Proposition 2.2 Si p est premier, et si $b, a > 0$ sont entiers, alors :

1. Ou bien : $(a, p) = 1$, ou bien : $p \mid a$.
2. Si p divise $a.b$, il divise a ou b .
- 2'. Si p divise un produit $a_1 \dots a_n$ de $n \geq 2$ entiers positifs, il divise l'un des a_j .
3. Si $p \mid a$ et si a est premier, alors $p = a$.

Démonstration : 1. $d := (a, p)$ divise p , donc vaut soit 1 soit p auquel cas $p \mid a$.

2. Si p ne divise pas a , on a : $(a, p) = 1$. Donc p divise b par le lemme d'Euclide.

On en déduit 2' par récurrence sur $n \geq 2$.

3. Si a est premier, $p > 1$ divise a . Donc $p = a$ \square

Théorème 2.3 (Euclide) L'ensemble des nombres premiers est infini.

Démonstration : Soit $p_1 < p_2 < \dots < p_r$ l'ensemble fini des nombres premiers majorés par p_r , et P leur produit. Nous allons montrer qu'il existe un nombre premier p tel que : $p_r < p \leq P$. Soit p un diviseur premier de $P+1$ (qui existe par la remarque 2.1). Puisque $P+1$ est premier avec P , chacun de ses diviseurs est premier avec chacun de ceux de P , donc avec chacun des $p_j, j = 1, \dots, p_r$. Donc $p \neq p_j, j = 1, \dots, r$ \square

Remarque 2.4 On ne connaît cependant pas de suite infinie de nombres premiers explicites. L'argument précédent montre par récurrence que $p_r < 2^{2^r}$. En fait : $p_r \sim r \cdot \log(r)$ (comme il résulte du "théorème des nombres premiers", dont la démonstration repose sur la fonction ζ d'Euler). On peut démontrer par des moyens élémentaires voir l'exercice 2.52) le "postulat de Bertrand" : pour tout entier $n > 0$, il y a un nombre premier compris entre n et $2n$, ce qui montre en particulier que $p_r < 2^r$. Le même type d'arguments élémentaires, dûs à Tchebychev, montre que $p_r = C_r \cdot r \cdot \log(r)$, avec $B > C_r > A$ compris entre deux constantes $A > 0$ et $B > 0$ (indépendantes de r).

Théorème 2.5 (Euclide) *Si $n > 1$ est entier, il s'écrit de manière unique comme produit de nombres premiers (en ordre croissant). Donc : $n = p_1^{r_1} \dots p_s^{r_s}$, avec $p_1 < p_2 < \dots < p_s$ premiers et $r_j > 0, \forall j$. (si $n = 1$, on prend : $s = 0$).*

Démonstration : Soit $p > 1$ le plus petit entier qui divise n : il est premier, par la remarque 2.1. Soit $n > m := n/p \geq 1$. Récurrence sur $n \geq 1$. On suppose le résultat vrai pour les entiers $1 \leq m < n$. On a donc existence et unicité de la décomposition pour m . On obtient ainsi l'existence pour n . Vérifions l'unicité. Si $n = p_1.p_2 \dots p_s$ est une seconde décomposition, avec $p_1 \leq p_2 \leq \dots \leq p_s$, la proposition précédente montre que $p = p_1$. En effet : p divisant le produit des p_j ne peut être premier avec tous. Il existe donc j tel que $(p, p_1) \neq 1$. On a donc $p = p_j$, puisque p et p_j sont premiers, par 2.2.3. Donc $j = 1$, par minimalité de p . Donc : $m = n/p = n/p_1 = p_2 \dots p_s$. L'unicité de la décomposition de m en facteurs premiers montre que $n = p_1 \dots p_s$ est l'unique décomposition de n en facteurs premiers \square

Proposition 2.6 *Pour tout $n \geq 1$, et tout nombre premier p , soit $v_p(n) \geq 0$ l'exposant de p dans la décomposition de n en produit de facteurs premiers. On a donc : $n = \prod_p p^{v_p(n)}$, le produit ayant un nombre fini de termes différents de 1.*

On a donc les propriétés suivantes, pour tous les entiers $m, n > 0$, et tous les nombres premiers p :

1. $v_p(m.n) = v_p(m) + v_p(n)$
2. $v_p(\text{pgcd}(m, n)) = \inf\{v_p(m), v_p(n)\}$.
3. $v_p(m \cap n) = \sup\{v_p(m), v_p(n)\}$.

Démonstration : La propriété 1. est évidente. Pour 2 et 3, observer que d divise n si et seulement si, pour tout p premier, $v_p(d) \leq v_p(n)$. Donc d divise m et n (resp. est un multiple de m et n) si et seulement si, pour tout p premier, on a : $v_p(d) \leq \inf\{v_p(m), v_p(n)\}$ (resp. $v_p(d) \geq \sup\{v_p(m), v_p(n)\}$).

Si l'on pose : $d' := \prod_p p^{\inf\{v_p(m), v_p(n)\}}$ et $m' := \prod_p p^{\sup\{v_p(m), v_p(n)\}}$, on voit donc que $d = (m, n)$ et $m' = (m \cap n)$, puisque d divise m et n (resp. est multiple de m et n) si et seulement si d divise d' (resp. est multiple de m') \square

Exemple 2.7 *Calculer $(1323, 3087)$ et $(1323 \cap 3087)$ par l'algorithme d'Euclide, et aussi en utilisant la décomposition en facteurs premiers.*

Remarque 2.8 *Les formules précédentes ne permettent de calculer (m, n) et $(m \cap n)$ que si l'on connaît leurs décomposition en produit de facteurs premiers. Cette décomposition est cependant si m, n sont grands, impossible à calculer en pratique (le nombre d'opérations nécessaires par les algorithmes connus est du même ordre de grandeur que $\sqrt{n} \cdot (\text{Log}n)^2$). L'algorithme d'Euclide est, au contraire, extrêmement rapide (ne nécessitant, au plus, que $2 \cdot \log_2(n)$ divisions).*

2.2 Exercices

Exercice 2.9 Redémontrer l'égalité $(a, b).(a \cap b) = a.b$ pour a, b entiers positifs, en utilisant l'expression de (a, b) et $a \cap b$ donnée en 2.6 en fonction des décompositions en facteurs premiers de a et b .

Exercice 2.10 Redémontrer l'exercice 1.31 en utilisant la décomposition en produit de facteurs premiers.

Exercice 2.11 Soit $a, b, c \in \mathbb{Z}$. Montrer que : $(c, (a \cap b)) = (c, a) \cap (c, b)$. Pour ceci, on pourra soit utiliser la décomposition en produit de facteurs premiers, soit se ramener d'abord au cas particulier où $(a, b) = 1$. Dans le premier cas, on sera ramené à montrer que si $m, n, p \geq 0$ sont trois entiers, alors :

$$\max(\inf(p, m), \inf(p, n)) = \inf(\max(p, m), \max(p, n)).$$

En déduire que : $(a \cap b, b \cap c, c \cap a) = ((a, b) \cap (b, c) \cap (c, a))$.

Exercice 2.12 Montrer que $(c \cap (a, b) = ((c \cap a), (c \cap b))$. Indication : procéder comme dans l'exercice précédent.

Exercice 2.13 1. Montrer que, en général, $c \cap (a, b) \neq (c, a) \cap (c, b)$. Donner un contre-exemple. Indication : déterminer v_p des deux membres, pour p premier arbitraire.

2. Montrer que, en général, $(c, (a \cap b)) \neq ((c \cap a), (c \cap b))$. Donner un contre-exemple. Indication : la même que pour 1.

Exercice 2.14 Soient p un nombre premier, $\alpha, \beta, \gamma \in \mathbb{N}$ et $u, v, w \in \mathbb{Z}$. Montrer que, si

$$p^{3\alpha}u + p^{3\beta+1}v + p^{3\gamma+2}w = p^{\alpha+\beta+\gamma}uvw,$$

alors $p|uvw$. (On pourra montrer que, dans le cas contraire, on aurait $\min(3\alpha, 3\beta + 1, 3\gamma + 2) = \alpha + \beta + \gamma + 1$ et que cette égalité est impossible).

Exercice 2.15 Soit p un nombre premier tel que $q := 2p + 1$ soit aussi premier. (Ex : $p = 2, 3, 5, 11$). Si l'équation $a^p + b^p = c^p$ a une solution entière a, b, c , alors abc est divisible par q . Vérifier pour $p = 2, q = 5$.

Exercice 2.16 Soit a, b, a', b' des entiers positifs ou nuls. On pose : $S := \inf\{a + a', b + b'\}$, $s := \inf\{a, b\} + \inf\{a', b'\}$, $s' := \inf\{a, b'\} + \inf\{a', b\}$.

1. Montrer que l'on a toujours : $s \leq S$ et $s' \leq S$. (Classer a et b , et a' et b').

2. On suppose que $a < b < b' < a'$. A quelle condition a-t'on : $a + a' < b + b'$? Montrer sur un exemple que ces 4 inégalités peuvent être simultanément satisfaites.

3. Montrer qu'alors $s' < s < S$.

Soit A, A', B, B' des entiers strictement positifs. On pose : $D := \text{pgcd}(AA', BB')$, $d := \text{pgcd}(A, B).\text{pgcd}(A', B')$, $d' = \text{pgcd}(A, B').\text{pgcd}(A', B)$.

4. Montrer que d et d' divisent D .

5. Les trois nombres D, d, d' peuvent-ils être deux-à-deux distincts ?

Exercice 2.17 Si a, b, c sont des entiers, montrer que $d := (a, c)$ divise $D = (ab, c)$ par deux méthodes (définition du pgcd comme générateur, et à l'aide de la décomposition en produit de facteurs premiers).

Exercice 2.18 Montrer par deux méthodes que, pour tous entiers a, b et $n > 0$, on a l'égalité : $\text{pgcd}(a^n, b^n) = (\text{pgcd}(a, b))^n$.

Exercice 2.19 Soit $n > 1$ entier. Le **radical** de n , noté $\text{rad}(n)$ est le produit des nombres premiers qui divisent n .

0. Montrer que si $m \mid n$, alors $\text{rad}(m) \mid \text{rad}(n)$, et qu'il existe une unique factorisation $n = n' \cdot m'$, avec $\text{rad}(m') = \text{rad}(m)$ et $(m', n') = (m, n') = 1$.

1. Montrer que n divise $\text{rad}(n)^k$ pour un entier $k > 0$ adéquat, et que $\text{rad}(n)$ divise n .

2. Montrer que $\text{rad}(n) = \text{rad}(m)$ si et seulement s'il existe des entiers k, ℓ tels que : $m \mid n^k$ et $n \mid m^\ell$.

3. On suppose que $\text{rad}(n) = \text{rad}(m)$ et que m divise n . Si $(a, m) = 1$, montrer que, pour tout entier b , $(a + b \cdot m, n) = 1$. Montrer que si $m \mid n$ et si $\text{rad}(m) \neq \text{rad}(n)$, il existe des entiers b tels que $(a + b \cdot m, n) \neq 1$. Indication : utiliser l'exercice ??.

*4. Montrer à l'aide du théorème Chinois, et de 0. et 3. ci-dessus, que si $m \mid n$ et si $(a, m) = 1$, il existe $b \in \mathbb{Z}$ tel que $(a + b \cdot m, n) = 1$.

Exercice 2.20 Montrer que si $2^p - 1$ est premier, alors p est premier. Les nombres $M_p := 2^p - 1$ avec p premier sont appelés "nombres de Mersenne". Parmi ceux-ci, M_p est premier pour $p = 2, 3, 5, 7, 11, 13$ (on a alors : $M_p = 3, 7, 31, 127, 2047, 8191$).

Exercice 2.21 Montrer que si $n > 1$, alors : $S_n := 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$ n'est pas un entier. (Si m est l'entier tel que $2^m \leq n < 2^{m+1}$, remarquer que $2^m \cdot S_n - 1$ est une somme de termes tous de la forme $\frac{a}{b}$, avec a pair et b impair.).

Exercice 2.22 Montrer qu'il existe une infinité d'entiers premiers de la forme $(4n + 3)$ ou $(6n + 5)$. (Considérer la forme des facteurs premiers d'entiers de la forme $N = k \cdot p_1 \dots p_r - 1$, avec $k = 4$, et 6 respectivement).

Exercice 2.23 Montrer qu'il existe une infinité d'entiers premiers de la forme $(8n + 5)$ ou $(4n + 1)$. On admettra pour cela que tout diviseur premier p d'une somme de deux carrés d'entiers est de la forme $p = 4k + 1$, et on considèrera un produit de la forme $N^2 + 2^2$, avec $N = p_1 \cdot p_2 \cdot \dots \cdot p_r$.

Exercice 2.24 Montrer que si $2^m + 1$ est premier, alors $m = 2^k$ pour un entier $k \geq 0$. On note $F_k := 2^{2^k} + 1$ le k -ième nombre de Fermat (qui pensait que tous étaient premiers, ce qui est vrai pour $k = 0, 1, 2, 3, 4$ pour lesquels $F_k = 3, 5, 17, 257, 65.537$, mais faux pour F_5 (voir exercice 2.28 ci-dessous)).

Exercice 2.25 Montrer que si $m > n$, alors $2^{2^n} + 1$ divise $2^{2^m} - 1$, et en déduire que $(2^{2^n} + 1, 2^{2^m} + 1) = 1$.

Exercice 2.26 Montrer que $F_0 \dots F_n = F_{n+1} - 2$. Redémontrer que les F_n sont deux à deux premiers entre eux.

Exercice 2.27 Soit p_r le r -ième nombre premier. Montrer (en utilisant 2.26) que $p_r \leq 2^{2^r} + 1$. En déduire que $\pi(n) \geq \log_2(\log_2(n))$, pour tout $n \geq 2$, si $\pi(n)$ est le nombre de nombres premiers au plus égaux à n .

Exercice 2.28 Pour $n \in \mathbb{N}$, on note $F_n := 2^{2^n} + 1$ le n -ième nombre de Fermat. On va montrer que F_5 n'est pas premier.

1. Sachant que $5^4 = 625$ et que $5 \cdot 2^7 = 640$, montrer que $5^4 \equiv -2^4$, que $5 \cdot 2^7 \equiv -1$ puis que $2^{32} \equiv -5^4 \cdot 2^{28} \equiv -1 [641]$. En déduire que 641 divise F_5 (donc que Fermat, croyant que tous les F_n sont premiers, se trompait). On verra plus tard pourquoi diviser F_5 par 641 dès le premier essai.

Exercice 2.29 Montrer que n a exactement $(r_1 + 1) \cdot (r_2 + 1) \cdot \dots \cdot (r_s + 1)$ diviseurs positifs si sa décomposition en facteurs premiers est : $n = p_1^{r_1} \dots p_s^{r_s}$.

Combien 945 a-t-il de diviseurs ? Quelle est leur somme, la somme de leurs carrés ?

Exercice 2.30 Soit n un entier impair.

1. Montrer qu'il y a une correspondance bijective entre les diviseurs $d > \sqrt{n}$ de n , et ceux tels que $d < \sqrt{n}$.

2. Montrer qu'il y a une correspondance bijective entre les diviseurs $d \geq \sqrt{n}$ de n , et les écritures de n comme différence $t^2 - s^2$ de deux carrés d'entiers.

3. Déterminer toutes les écritures de 945 comme différence de deux carrés d'entiers positifs.

4. Factoriser $n = 8633, 8645, 8463, 8455, 8439$, sachant que ces entiers n ont un facteur proche de \sqrt{n} .

5. Montrer que si n a un diviseur d tel que $0 < |d - \sqrt{n}| < \sqrt{2} \cdot \sqrt[4]{n}$, alors $([\sqrt{n}] + 1)^2 - n$ est un carré d'entier. (Montrer que $|\frac{1}{2} \cdot (d + \frac{\sqrt{n}}{d}) - \sqrt{n}| < \frac{\alpha^2}{2\sqrt{n}}$ si $d = \sqrt{n} + \alpha$).

Exercice 2.31 Si $a, d \in \mathbb{Z}$ sont non nuls, il y a dans la suite $N_j := a + j \cdot d, j \geq 0$ une infinité de termes ayant les mêmes facteurs premiers. (Si $(a, d) = 1, a > d$, considérer les N_j avec $j := \frac{a}{d} \cdot (a^{\varphi(d) \cdot k} - 1)$).

Exercice 2.32 Soit $P(X)$ un polynôme à coefficients entiers. Si $a > 0, b > 0$ sont entiers tels que $P(a) = p$ et $P(b) = q$ soient premiers, montrer que si $c \equiv a[p]$ et $c \equiv b[q]$, alors $P(c) \equiv 0[pq]$. $P(X)$ peut-il ne prendre que des valeurs qui sont des nombres premiers ?

Exercice 2.33 Si a, b, c sont entiers, $b \geq 2$, l'ensemble des nombres premiers divisant l'un au moins de tous les nombres $N_k := a \cdot b^k + c, k \geq 0$, est infini. (modulo tout $n > 1$ premier avec b , les N_k forment une suite périodique).

Exercice 2.34 Soit a, b, c des entiers non nuls, et $d := (a, b)$ et $e := (a, c)$ les PGCD. Si a divise $b \cdot c$, montrer que a divise $c \cdot d$ et $b \cdot e$. (Considérer $a' := \frac{a}{d}$ et $b' := \frac{b}{d}$).

2.3 *Décomposition en facteurs premiers de n !

Théorème 2.35 Soit $n > 0$ un entier, et : $n! = 1.2.3.\dots.n$. Pour tout nombre premier p , on a : $v_p(n!) = \sum_{j=1}^{j=+\infty} \left[\frac{n}{p^j} \right]$.

Cette somme est finie, les termes étant nuls pour j tel que : $p^j > n$.

On en déduit l'encadrement : $\left[\frac{n-1}{p-1} - \log_p(n) \right] \leq v_p(n!) \leq \left[\frac{n-1}{p-1} \right]$ (voir exercice 2.45).

Première démonstration : Soit k le plus grand entier tel que $p^k \leq n < p^{k+1}$. Le nombre c_j des entiers $1 \leq m \leq n$ qui sont divisibles par p^j est donc égal à $\left[\frac{n}{p^j} \right] = c_j$ pour tout $j \geq 1$, et vaut en particulier 0 si $j \geq k+1$. Le nombre b_j des entiers $1 \leq m \leq n$ divisibles par p^j mais pas par p^{j+1} , c'est-à-dire tels que $v_p(m) = j$ est donc égal à $c_j - c_{j+1}$ pour tout $j \geq 1$. On a donc :

$$v_p(n!) = \sum_{j=1}^{j=k} j \cdot b_j = \sum_{j=1}^{j=k} j \cdot (c_j - c_{j+1}) = \sum_{j=1}^{j=k} (j \cdot c_j - (j+1) \cdot c_{j+1}) + \sum_{j=2}^{j=k} c_j = c_1 + \sum_{j=2}^{j=k} c_j = \sum_{j=1}^{j=k} \left[\frac{n}{p^j} \right].$$

Deuxième démonstration : Elle est vraie pour $n = 1$ (et tout p). On procède par récurrence sur n , p étant fixé. Si $(n+1) = p^k \cdot m$, avec p ne divisant pas m , alors : $v_p((n+1)!) = v_p(n!) + v_p(n+1) = v_p(n!) + k = \sum_{j=1}^{j=+\infty} \left[\frac{n}{p^j} \right] + k$ par hypothèse de récurrence. Le lemme 2.36 ci-dessous montre alors que $\left[\frac{n+1}{p^j} \right] = \left[\frac{n}{p^j} \right]$ si $j > k$ et que $\left[\frac{n+1}{p^j} \right] = \left[\frac{n}{p^j} \right] + 1$ si $1 \leq j \leq k$. Donc $\sum_{j=1}^{j=+\infty} \left[\frac{n+1}{p^j} \right] = \sum_{j=1}^{j=+\infty} \left[\frac{n}{p^j} \right] + k \quad \square$

Lemme 2.36 Si $0 < m$ et $0 < n$ sont entiers, alors $\left[\frac{n+1}{m} \right] = \left[\frac{n}{m} \right]$ si m ne divise pas $(n+1)$ et $\left[\frac{n+1}{m} \right] = \left[\frac{n}{m} \right] + 1$ si m divise $(n+1)$.

Démonstration : Ecrivons $(n+1) = q \cdot m + r$, q, r étant quotient et reste de la division euclidienne de $(n+1)$ par m .

On suppose $m \geq 2$, car l'énoncé est évident si $m = 1$.

Alors $\frac{n+1}{m} = q + \frac{r}{m}$. Donc $\frac{n}{m} = q + \frac{r-1}{m}$, avec : $\frac{r-1}{m} < \frac{r}{m} < 1$.

Si $r \geq 1$, $\frac{r-1}{m} \geq 0$. Donc $q = \left[\frac{n}{m} \right] = \left[\frac{n+1}{m} \right]$.

Si $r = 0$, $\frac{n}{m} = \frac{n+1}{m} - \frac{1}{m} = q - \frac{1}{m} = (q-1) + \frac{m-1}{m}$. Donc $\left[\frac{n}{m} \right] = q-1 = \left[\frac{n+1}{m} \right] - 1 \quad \square$

Nous donnons maintenant une méthode rapide de calcul du second membre de l'égalité de 2.35, évitant les divisions de n par p^j .

Corollaire 2.37 Pour tout $n > 1$, et tout nombre premier p , $v_p(n!) = a_1 + a_2 + \dots + a_k + \dots$, avec $a_1 := \left[\frac{n}{p} \right]$, et $a_{j+1} = \left[\frac{a_j}{p} \right]$ pour $j = 1, 2, \dots, (k-1)$. (Les termes a_j sont nuls si $j > k = \left[\log_p(n) \right] = \left[\frac{\log n}{\log p} \right]$).

Exemple 2.38 $v_2(100!) = 50+25+12+6+3+1 = 97$, $v_3(100!) = 33+11+3+1 = 48$, $v_5(100!) = 20 + 4 = 24$, $v_7(100!) = 14 + 2 = 16$.

Démonstration (de 2.37) : Le lemme suivant montre que $a_{j+1} := \left[\frac{a_j}{p} \right] = \left[\frac{a_j}{p} \right]$, pour tout $j > 0$, par récurrence sur $j \quad \square$

Lemme 2.39 Pour tous entiers strictement positifs n, d, d' , on a : $[\frac{n}{dd'}] = [\frac{[\frac{n}{d}]}{d'}]$

Démonstration : Si $n = qdd' + r$ est la division de n par dd' , on a $q = [\frac{n}{dd'}]$, et $0 \leq r < dd'$. Donc $n = (qd' + q')d + s$, si $r = q'd + s$ est la division de r par d , avec $0 \leq s < d$, et $q' < d'$, puisque $r < dd'$. Donc $[\frac{n}{d}] = qd' + q'$, et $[\frac{[\frac{n}{d}]}{d'}] = q \square$

Corollaire 2.40 (Legendre) Soit $n > 0$ un entier, et p un nombre premier p .

Soit $n = \sum_{j=0}^{j=k} t_j \cdot p^j$, avec : $0 \leq t_j \leq (p-1)$ l'écriture de n en base p . On note $t_p(n) := \sum_{j=0}^{j=k} t_j$ la somme des coefficients de l'écriture de n en base p .

$$\text{Alors : } v_p(n!) = \frac{n - (\sum_{j=0}^{j=k} t_j)}{p-1} = \frac{n - t_p(n)}{p-1}.$$

Démonstration : On utilise les notations de 2.37. On a alors, par divisions euclidiennes par p , dont les restes sont notés : s_0, s_1, \dots, s_k :

$$n = a_1 \cdot p + s_0, a_1 = a_2 \cdot p + s_1, \dots, a_j = a_{j+1} \cdot p + s_j, \dots, a_k = s_k, \text{ pour } j = 0, 1, \dots, k.$$

On a donc, par récurrence sur j : $n = a_{j+1} \cdot p^{j+1} + s_j \cdot p^j + \dots + s_1 \cdot p + s_0$, pour $j \leq k$. Donc $n = s_k \cdot p^k + \dots + s_j \cdot p^j + \dots + s_1 \cdot p + s_0$. Donc $s_j = t_j$ pour tout j . On note : $a_0 := n$.

De plus, d'après 2.37, $v_p(n!) = \sum_{j=1}^{j=k} a_j = \sum_{j=1}^{j=k} (\frac{a_{j-1}}{p} - \frac{s_{j-1}}{p}) = (\frac{n+a_1+\dots+a_k}{p}) - (\frac{s_0+\dots+s_k}{p}) = \frac{n-t_p(n)}{p} + \frac{v_p(n!)}{p} = v_p(n!)$, d'où l'on déduit l'égalité de Legendre \square

Corollaire 2.41 Pour tous $n > 0$ et $0 \leq m \leq n$, on a :

1. $C_n^m := \frac{n!}{m!(n-m)!}$ est entier ³.
2. Si p est premier, et si $0 < m < p$, alors C_p^m est divisible par p .

Démonstration : 1. $[\frac{n}{p^j}] \geq [\frac{m}{p^j}] + [\frac{n-m}{p^j}]$, pour tout $j > 0$. (Plus généralement : $[x+y] \geq [x] + [y]$ pour tous $x, y \in \mathbb{R}$, positifs). Donc $v_p(C_n^m) \geq 0$, pour tout p , et $C_n^m \in \mathbb{Q}$ est donc entier.

2. En effet : p divise $p!$, mais ne divise ni $m!$ ni $(p-m)!$ puisqu'il ne divise aucun des facteurs, et il ne divise donc pas leur produit (puisque premier avec chacun d'eux). Donc il divise l'entier C_p^m , puisque $p! = C_p^m \cdot m! \cdot (p-m)!$ \square

Corollaire 2.42 Soit p premier, et $r \geq 1$ un entier.

1. Pour tout entier k tel que $1 \leq k \leq p^r - 1$, $C_{p^r}^k$ est divisible par p . Plus précisément : $1 \leq v_p(C_{p^r}^k) \leq r$.

2. Si $0 \leq k \leq p^r$ est entier, et si $k = p^s \cdot \ell$, avec $0 \leq s \leq r$, et $(\ell, p) = 1$, alors $v_p(C_{p^r}^k) = r - s$.

Démonstration : 1. Les deux premières assertions résultent de ce que : $v_p((p^r)!) = [p^{r-1}] + [p^{r-2}] + \dots + [p] + 1$, et $v_p((p^r - k)!) = [\frac{p^r - k}{p}] + [\frac{p^r - k}{p^2}] + \dots + [\frac{p^r - k}{p^{r-1}}]$, ainsi que : $v_p(k!) = [\frac{k}{p}] + [\frac{k}{p^2}] + \dots + [\frac{k}{p^{r-1}}]$.

Il suffit donc d'appliquer l'encadrement $[x] + [y] \leq [x+y] \leq [x] + [y] + 1$ pour $x = \frac{k}{p^j}, y = \frac{p^r - k}{p^j}$ pour $j = 1, \dots, r-1$.

³On en donne une démonstration arithmétique, indépendante de son interprétation comme cardinal de l'ensemble des parties à m éléments d'un ensemble ayant n éléments.

2. On obtient le résultat par récurrence sur $k \geq 1$, à l'aide de l'égalité : $C_{p^r}^{k+1} = \binom{n-k}{k+1} \cdot C_{p^r}^{k-1}$, puisque si $k = p^s \cdot \ell$, avec $(p, \ell) = 1$, alors l'égalité précédente montre que : $v_p(C_{p^r}^{k+1}) = v_p(C_{p^r}^k) + v_p(p^r - k) - v_p(k+1) = v_p(C_{p^r}^k) + v_p(p^r - p^s \cdot \ell) - v_p(k+1) = (r - s) + s - v_p(k+1) = r - v_p(k+1)$, ce qui est l'égalité annoncée. (On a utilisé le fait que $v_p(p^r \cdot m - p^s \cdot \ell) = r - s$ si $r \neq s$ et si $(m, p) = 1$). \square

Remarque 2.43 Pour tous m, n , et tout nombre premier p , la puissance exacte de p divisant C_n^m est le nombre de retenues dans l'addition des écritures de m et $n - m$ en base p . C'est un résultat de Kummer basé sur celui de Legendre ci-dessus.

2.4 Exercices

Exercice 2.44 Soit p premier. Pour tout nombre rationnel $x = \frac{u}{v}$, avec $u > 0$ et $v > 0$ entiers, on pose $v_p(x) := v_p(u) - v_p(v) \in \mathbb{Z}$. Si $x = 0$, on pose : $v_p(0) := +\infty$, et si $x < 0$, on pose : $v_p(x) = v_p(-x)$.

1. Montrer que la fonction v_p est ainsi bien définie (indépendante de la représentation de x comme quotient de deux entiers positifs si $x > 0$).

2. Montrer que $v_p(x \cdot y) = v_p(x) + v_p(y)$ pour tous $x, y \in \mathbb{Q}$ (on pose, bien sûr : $a + (+\infty) = +\infty$ si $a \in \mathbb{Z}$ ou si $a = +\infty$).

3. Montrer que $v_p(x + y) \geq \inf\{v_p(x), v_p(y)\}$ pour tous $x, y \in \mathbb{Q}$, avec égalité si $v_p(x) \neq v_p(y)$ (on pose, bien sûr : $\inf\{a, +\infty\} = a$ si $a \in \mathbb{Z}$ ou si $a = +\infty$).

Exercice 2.45 Montrer que : $[\frac{n-1}{p-1} - \log_p(n)] \leq v_p(n!) \leq [\frac{n-1}{p-1}]$, pour tous $n > 1$ et p premier.

Exercice 2.46 1. Montrer que $v_p(n!) = \sum_{j \geq 0} [\frac{n}{p^j}]$, pour tout n et tout p premier.

2. Déterminer les exposants de 2, 3, 5, 7 dans la décomposition de $100!$ en produit de facteurs premiers. Décomposer alors $100!$ en facteurs premiers.

3. Montrer que $v_2(n!) = n - S_2(n)$, si $S_2(n)$ est la somme des chiffres de l'écriture de n en base 2. Vérifier ainsi le calcul précédent de $v_2(100!)$.

4. Calculer $v_p(n!)$ pour p premier arbitraire, par une formule analogue : $v_p(n!) = \frac{n - S_p(n)}{p-1}$.

Exercice 2.47 Si $m = a_1 + a_2 + \dots + a_k$ est une somme d'entiers $a_j \geq 1$, montrer par récurrence sur $k \geq 1$ que $a := \frac{m!}{a_1! a_2! \dots a_k!}$ est entier. (Écrire a comme produit de $(k-1)$ coefficients binomiaux si $k \geq 2$).

Exercice 2.48 Si $x \in \mathbb{Q}$, on pose : $f(x) := [x] - [\frac{x}{2}] - [\frac{x}{3}] - [\frac{x}{4}] + [\frac{x}{12}] \in \mathbb{Z}$, et : $\{x\} := x - [x] \in [0, 1[$.

1. Montrer que $f(x) = g(x) := \{\frac{x}{2}\} + \{\frac{x}{3}\} + \{\frac{x}{4}\} - \{\frac{x}{12}\} - \{x\} > -1$, si $x \in \mathbb{Z}$. (Montrer que $f(x) - g(x) = 0$ pour tout $x \in \mathbb{Q}$, en utilisant l'égalité : $1 + \frac{1}{2} = \frac{1}{2} + \frac{1}{2} + \frac{1}{2}$, puis remarquer que $g(x) > 1$ si $x \in \mathbb{Z}$. Conclure en remarquant que $f(x) \in \mathbb{Z}$).

2. Montrer que $f(x) \geq 0$ si $x \in \mathbb{Q}$. (Montrer que $f(x) = f([x])$ en utilisant l'exercice 1.5).

3. Montrer que $\frac{(12n)!n!}{(3n)!(4n)!(6n)!}$ est entier, pour tout entier $n \geq 1$.
4. Comparer ce résultat avec celui de l'exercice 2.47.
5. Montrer, de la même façon, que, pour tout entier $n \geq 1$, a_n et b_n sont entiers :
 $a_n := \frac{(30.n)!n!}{(6n)!(10n)!(15n)!}$ et $b_n := \frac{(210.n)!n!}{(2n)!(10n)!(21n)!(70n)!(105.n)!}$ sont entiers. Comparer ces résultats avec celui de l'exercice 2.47

Exercice 2.49 On rappelle que, d'après 2.40, $v_p(n!) = \frac{n-t_p(n)}{p-1}$ si $t_p(n)$ est la somme des coefficients de l'écriture de n en base p , premier arbitraire.

1. Si $N_n := \frac{(11n)!n!n!}{(3n)!(4n)!(6n)!}$, montrer que $v_2(N_n) = 2.t_2(3n) - t_2(n) - t_2(11n)$. (Observer que $t_2(2n) = t_2(n)$).
2. Montrer que $t_2(11n) = m$ si $11n = 2^m - 1$.
3. On choisit $n = \frac{2^{10}-1}{11} = 93$. Montrer que $v_2(N_{93}) = -5$, et en déduire que N_{93} n'est pas entier.

Exercice 2.50 Montrer, par la méthode de l'exercice 2.48, que si N, a_1, \dots, a_k sont des entiers strictement positifs tels que l'on ait l'égalité : $(*) 1 + \frac{1}{N} = \sum_1^k \frac{1}{a_j}$, alors :

1. $f(x) := [x] - [\frac{x}{a_1}] - [\frac{x}{a_2}] - \dots - [\frac{x}{a_k}] + [\frac{x}{N}] \geq 0$
2. Pour tout entier $n \geq 1$, tel que $\frac{Nn}{a_j}$ soit entier pour tout $j = 1, \dots, k$, le rationnel $b_n := \frac{(Nn)!n!}{((\frac{Nn}{a_1})!) \dots ((\frac{Nn}{a_k})!)}$ est entier.
3. Montrer que si d_1, \dots, d_k sont des diviseurs de N tels que $d_1 + \dots + d_k = N + 1$, on a l'égalité $(*)$, avec $a_j = \frac{N}{d_j}, j = 1, \dots, k$, et que $b_n = \frac{(Nn)!n!}{(d_1n)! \dots (d_kn)!}$ est entier pour tout $n \geq 1$.

Exercice 2.51 On montre dans cet exercice comment trouver des suites N, a_1, a_2, \dots, a_k satisfaisant la condition $(*)$ de l'exercice 2.50.

1. Si $(\sum_1^{k-1} \frac{1}{a_j}) + \frac{1}{b} = 1$, montrer que : $(\sum_1^{k-1} \frac{1}{a_j}) + \frac{1}{b-1} = 1 + \frac{1}{N}$, avec : $N := b.(b-1)$, et montrer que $(\sum_1^{k-1} \frac{1}{a_j}) + \frac{1}{a_k} + \frac{1}{b'} = 1$, avec : $a_k := b+1$ et $b := b.(b+1)$.
 Indication : utiliser l'égalité : $\frac{1}{b} = \frac{1}{b+1} + \frac{1}{b.(b+1)}$.

2. On choisit $k = 1, a_1 = b = 2$. On définit la suite $a_n, n \geq 1$, par récurrence : $a_{k+1} = a_k.(a_k - 1)$ si $k \geq 1$. Calculer les 5 premiers termes, et montrer que, pour tout $n \geq 2$, on a les propriétés suivantes :

- 2a. $a_{n+1} = a_1 \dots a_n + 1$.
- 2b. $(\sum_1^n \frac{1}{a_j}) = 1 - \frac{1}{a_{n+1}}$
- 2c. $(\sum_1^n \frac{1}{a_j}) + \frac{1}{a_{n+1}-1} = 1$
- 2d. $(\sum_1^n \frac{1}{a_j}) + \frac{1}{a_{n+1}-2} = 1 + \frac{1}{(a_{n+1}-1).(a_{n+1}-2)}$
3. Effectuer une étude analogue avec $k \geq 2, a_1 = a_2 = \dots = a_k = b = (k+1)$.

Exercice 2.52 L'objectif des exercices qui suivent est de démontrer le "postulat de Bertrand" : si $n > 0$ est entier, il y a entre n et $2n$ au moins un nombre premier.

1. Montrer que $\frac{p_{2n}}{p_n}$ divise C_{2n}^n
2. Montrer que $\frac{2^{2n}}{2+1} \leq C_{2n}^n \leq \frac{2^{2n}}{2}$. Indication : $2^{2n} = (1+1)^{2n}$.

Exercice 2.53 Pour tout $n > 1$, on note P_n le produit des nombres premiers au plus égaux à n . Montrer que $P_n \leq 4^n, \forall n > 0$. Indication : procéder par récurrence, distinguer les cas n pair et impair, et utiliser l'exercice précédent.

Exercice 2.54 * Soit p premier. Montrer que :

0. $v(p, n) = \sum_{j \geq 0} \{[2n/p^j] - 2[n/p^j]\}$, $v(p, n)$ étant l'exposant de p dans la décomposition en produit de facteurs premiers de C_{2n}^n . Montrer que :

1. $v(p, n) \leq [\text{Log}(2n)/\text{Log}(p)]$, qui est le plus grand des entiers j tels que $p^j \leq 2n$. (Indication : tous les termes de la somme valent 0 ou 1).

2. $p^{v(p, n)} \leq 2n$, pour tout p .

3. Si $2n/3 < p \leq n$, alors $v(p, n) = 2 - 2 = 0$.

Si J est un intervalle de \mathbb{R} , soit P_J le produit des $p^{v(p, n)}$, pour p premier dans J . On note ainsi $P_1 = P[0, \sqrt{2n}]$, $P_2 := P_{[1, 2n/3]}$, $P_3 := P_{[2n/3, n]}$, et $P_4 = P_{[n, 2n]}$. On a donc $C_{2n}^n = P_1.P_2.P_3.P_4$.

Le postulat de Bertrand équivaut donc à : $P_4 > 1$ pour tout $n > 0$. Montrer à l'aide des questions précédentes que :

4. $P_1 \leq 2n^{\sqrt{2n}}$.

5. $P_2 \leq 4^{2n/3}$.

6. $P_3 = 1$.

7. $4^n/(2n+1) \leq C_{2n}^n \leq (2n)^{\sqrt{2n}}.4^{2n/3}.P_4$.

8. $P_4(n) = P_4 \geq \frac{4^{n/3}}{(2n+1).(2n)^{\sqrt{2n}}} = \varphi(n)$.

9. $\text{Log}P_4(n) = \text{Log}P_4 \geq \frac{2n.\text{Log}2}{3} \cdot \left\{ 1 - \left(\frac{6}{\text{Log}2}\right) \cdot \left(\frac{\text{Log}\sqrt{2n}}{\sqrt{2n}} + \frac{\text{log}2n}{2n}\right) \right\} = \psi(n)$.

10. Montrer que $\psi(n)$ tend vers $+\infty$ avec n .

11. En déduire que le postulat de Bertrand est vrai pour tout $n \geq n_0$ assez grand.

12. Montrer que $\text{Log}(P_4) = \text{Log}(P_4(n)) \geq \frac{n.\text{Log}4}{4}$ pour tout $n \geq n_1$ assez grand.

13. Montrer que le nombre de nombres premiers compris entre n et $2n$ est au moins égal à $\frac{n.\text{Log}4}{\text{Log}(2n).4}$ pour tout $n \geq n_1$ assez grand.

14. Déterminer des valeurs explicites de n_0 et n_1 en posant : $2n = 2^t$.

15. En déduire le Postulat de Bertrand en choisissant une suite de nombres premiers p_k telle que $p_1 = 2, p_{k+1} \leq 2.p_k$ pour $k \leq \text{Log}_2(n_0)$.

3 CONGRUENCES.

3.1 Congruences modulo n , Opérations.

Congruences : On dit que les entiers $a, a' \in \mathbb{Z}$ sont **congrus modulo n** , $n > 0$ un entier fixé, (ce qui est noté : $a \equiv a' [n]$) si $a - a'$ est divisible par n , c'est une relation d'équivalence.

De plus : a et a' sont congrus modulo n si et seulement s'ils ont même reste dans la division euclidienne par n . Il y a donc n classes d'équivalence pour cette relation, représentées par les n restes $r \in \{0, 1, \dots, (n-1)\}$ possibles.

Soit $n \geq 2$ un entier, et $a, b \in \mathbb{Z}$. On note $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$, et $p_n = p : \mathbb{Z} \rightarrow \mathbb{Z}_n$ la projection naturelle, qui associe à a le reste, noté \bar{a} (ou $\bar{a}^{(n)}$ si l'on veut préciser n) de sa division euclidienne par n .

On en déduit les propriétés fondamentales suivantes :

Théorème 3.1 *Si $a, a', b, b' \in \mathbb{Z}$, et si $a \equiv b[n]$, et si $a' \equiv b'[n]$, alors :*

1. $a + a' \equiv b + b'[n]$
2. $a.a' \equiv b.b'[n]$
3. $a^k \equiv b^k, \forall k \geq 0$, entier
4. Si $c_0 + c_1.X + \dots + c_d.X^d = P(X) \in \mathbb{Z}[X]$ est un polynôme à coefficients entiers, alors : $P(a) \equiv P(b)[n]$.

Corollaire 3.2 *On peut munir \mathbb{Z}_n de deux opérations, notées aussi $+$ et \times , en posant, pour tous $a, a' \in \mathbb{Z}$:*

1. $\bar{a} + \bar{a}' := \overline{a + a'} = \bar{a} + \bar{a}'$
2. $\bar{a} \times \bar{a}' := \overline{a \times a'}$
3. $\bar{a} \times (\bar{b} + \bar{c}) = \bar{a} \times \bar{b} + \bar{a} \times \bar{c}$, pour tous $a, b, c \in \mathbb{Z}_n$.

On a alors aussi, pour tous $a \in \mathbb{Z}, k \geq 0$, entier :

4. $(\bar{a})^k = \overline{a^k}$. (\bar{a}^k est le produit, dans \mathbb{Z}_n , de k termes tous égaux à \bar{a}).
5. Si on note $\bar{P}(X) := \bar{c}_0 + \bar{c}_1.X + \dots + \bar{c}_d.X^d \in \mathbb{Z}_n[X]$ le polynôme à coefficients dans \mathbb{Z}_n déduit de $P(X)$ (dans 3.1.(4). ci-dessus) en y remplaçant ses coefficients par leurs classes dans \mathbb{Z}_n , alors pour tout $a \in \mathbb{Z}$, on a : $\bar{P}(a) = \bar{P}(\bar{a})$.

Ces opérations ne dépendent pas des représentants a, a' des classes \bar{a}, \bar{a}' choisis pour les définir ⁴.

Exemple 3.3 1. Dans \mathbb{Z}_7 , on a : $\bar{3} + \bar{5} = \bar{1} = \bar{3} \times \bar{5}$.

2. Tout $\bar{a} \in \mathbb{Z}_n$ a un opposé, $-\bar{a}$ pour $+$: $-\bar{a} = \overline{-a} = \overline{n-a}$.

3. Dans \mathbb{Z}_9 , on a : $\overline{10^k} = \bar{1}, \forall k \geq 0$.

4. Dans \mathbb{Z}_{11} , on a : $\overline{10^k} = (-1)^k, \forall k \geq 0$.

Exemple 3.4 *Soit $n > 0$ un entier, et $t_{2d}.t_{2d-1} \dots .t_1.t_0$ son écriture décimale (les t_j étant donc entiers et compris entre 0 et 9, et t_{2d} éventuellement nul). Alors les restes des divisions euclidiennes de n par 3, 9, 11 sont, respectivement, les restes des divisions euclidiennes par 3, 9, 11 des entiers :*

$$t_{2d} + t_{2d-1} + \dots + t_1 + t_0,$$

$$t_{2d} + t_{2d-1} + \dots + t_1 + t_0,$$

$$t_{2d} - t_{2d-1} + \dots + (-1)^j.t_j + \dots - t_1 + t_0.$$

Par exemple, le reste de la division euclidienne par 11 de 74351985 est aussi celui de : $(5 - 8 + 9 - 1 + 5 - 3 + 4 - 7)$, soit 4.

De même, le reste des divisions euclidiennes par 9 et 11 de $k = 31782$ est 3, donc $(k - 3) = 31779$ est divisible par 99.

⁴Ces propriétés peuvent être résumées en disant que $(\mathbb{Z}_n, +, \times)$ est un anneau commutatif de cardinal n , et que $p_n : \mathbb{Z} \rightarrow \mathbb{Z}_n$ est un morphisme d'anneaux.

3.2 exercices

Exercice 3.5 Montrer que 7 divise $3^{105} + 4^{105}$

Exercice 3.6 Montrer que 3 divise a et b si et seulement si 3 divise $a^2 + b^2$.

Exercice 3.7 Montrer que 6 divise $a + b + c$ si et seulement si 6 divise $a^3 + b^3 + c^3$.

Exercice 3.8 Calculer le reste de la division euclidienne par 17 de $(1035125)^{5642}$.

Exercice 3.9 Calculer le reste de la division euclidienne par 18 de $(1823)^{242}$.

Exercice 3.10 Calculer le reste de la division euclidienne par 20 de $(2222)^{321}$.

Exercice 3.11 Montrer que $n^7 \equiv n[7]$, pour tout $n \in \mathbb{Z}$, et ensuite que $n^7 \equiv n[42]$, pour tout $n \in \mathbb{Z}$.

Exercice 3.12 Si quelqu'un vous donne le nombre $n = 13.j + 14.m$, où $1 \leq j \leq 31$ (resp. $1 \leq m \leq 12$) est son jour (resp. mois) de naissance, pouvez-vous retrouver j et m ? Si oui, comment?

Exercice 3.13 1. $N = 1387496611000$ est-il une puissance quatrième (ie : de la forme $N = a^4, a \in \mathbb{Z}$) ?

2. Dans le système décimal, quels sont les chiffres des unités possibles d'un nombre entier impair N de la forme $N = a^4$, si $a \in \mathbb{Z}$?

3. Même question si N est pair.

4. Si $N = a^4$ est divisible par 5, quel sont les 4 derniers chiffres de N en écriture décimale. ?

Exercice 3.14 Calculer le reste de la division de 19^{59} par 77.

Exercice 3.15 Calculer les restes des divisions de 23^{39} et 23^{38} par 82.

Exercice 3.16 Montrer que, pour tout entier n , 360 divise $n^2 \cdot (n^2 - 1)(n^4 - 16)$.

Exercice 3.17 Montrer que, pour tous entiers a, b et $n > 0$, $\text{pgcd}(a^n, b^n) = \text{pgcd}(a, b)^n$.

Exercice 3.18 Calculer le reste de la division de 27^{103} par 143.

Exercice 3.19 Calculer le reste de la division de 10^{100} par 247.

Exercice 3.20 Calculer le reste de la division de 55555^{55555} par 7.

Exercice 3.21 Calculer le reste de la division de 3^{683} par 245.

Exercice 3.22 Calculer le reste de la division de 3^{164} par 88.

Exercice 3.23

1. Montrer que si $p - 1, p$, premier, divise $k - 1$, alors $a^k \equiv a[p]$, et $ab(a^k - b^k) \equiv 0[p]$ quels que soient $a, b \in \mathbb{Z}$.
2. Dédurre de 1. que $2.3.5.7.11.13.31.61 = 56786730$ divise $ab(a^{60} - b^{60})$.
3. Formuler des résultats analogues si l'exposant 60 est remplacé par 6, 12, 24 ou 30.

Exercice 3.24 Montrer que, pour tout $n \in \mathbb{Z}$, $3^{n+3} \equiv 4^{4n+2}[11]$.

Exercice 3.25 Déterminer le reste de la division de 37^n par 11 pour $n \in \mathbb{N}$. Combien de cas faut-il considérer ?

Exercice 3.26 Montrer que $n^5 - n$ est toujours divisible par 30 si $n \in \mathbb{Z}$.

Exercice 3.27 Déterminer les nombres de trois chiffres congrus à 4 modulo 7, 9 et 11.

Exercice 3.28 Trouver le reste de la division de 6647^{362} par $n = 7785562197230017200 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 181$.

Exercice 3.29 Montrer que $\overline{13}$ est inversible dans \mathbb{Z}_{31} , et déterminer son inverse.

Exercice 3.30 Déterminer les entiers $n \in \mathbb{Z}$ satisfaisant les systèmes de congruences A , puis B suivants :

- A. $2n \equiv 3[11]$ et $3n \equiv 2[17]$.
- B. $2n \equiv 3[11]$, $3n \equiv 2[17]$, et $5n \equiv 4[13]$.

Exercice 3.31 Déterminer (presque sans calcul) le reste de la division euclidienne de N par 99 si : $N = (359141)^{359141}$.

Exercice 3.32 Soit $n \equiv 1[6]$ un entier positif. On pose : $N = n^2 + n + 1$. Montrer que :

1. $N \equiv 0[3]$.
2. $(n + 1)^{(n+1)} \equiv n^n[N]$.
3. $3 \cdot (n + 1)^{(n+1)} \equiv 3 \cdot n^n[N^2]$.
4. A-t'on : $(n + 1)^{(n+1)} \equiv n^n[N^2]$?

Exercice 3.33 Si n est un entier, quels sont les restes possibles de la division de n^2 par 10 ? Le nombre 385442732 est-il un carré ? Le nombre 385442739 (resp. 385442765) est-il un carré ? (Reste modulo 4 (resp. 8)). Quels sont les restes possibles d'un carré d'entier modulo 10, modulo 4, modulo 8 ?

Exercice 3.34 Si $a \in \mathbb{Z}$ a pour reste 7 dans sa division par 8, montrer que a n'est pas somme de trois carrés d'entiers.

Exercice 3.35 Soit $F_k := 2^{2^k} + 1$ pour $k \geq 0$ entier le k -ième nombre de Fermat. Montrer que $F_k \equiv 7[10]$ pour $k \geq 2$. (Remarquer que $F_{k+1} = (F_k - 1)^2 + 1$).

Exercice 3.36 Soit $m > 0$ entier, et N la plus grande puissance de 2 qui divise $[(1 + \sqrt{3})^{2m+1}]$. Montrer que $N = 2^{m+1}$. (Remarquer que $[(1 + \sqrt{3})^{2m+1}] = (1 + \sqrt{3})^{2m+1} + (1 - \sqrt{3})^{2m+1}$. Noter ensuite que : $(1 + \sqrt{3}) \cdot (4 + 2\sqrt{3})^m + (1 - \sqrt{3}) \cdot (4 - 2\sqrt{3})^m = 2^m \cdot A$, avec $A = (1 + \sqrt{3}) \cdot (2 + \sqrt{3})^m + (1 - \sqrt{3}) \cdot (2 - \sqrt{3})^m$, et A est de la forme : $2(a + b\sqrt{3}) + (1 + \sqrt{3}) \cdot (\sqrt{3})^m + 2(a - b\sqrt{3}) + (1 - \sqrt{3}) \cdot (-\sqrt{3})^m$ est donc divisible par 2, mais pas par 4).

Exercice 3.37 Si $\bar{2} = a^2$ et $\overline{(-1)} = b^2$ sont des carrés dans \mathbb{Z}_n , n impair, montrer que $(1 + b)^2 = 2b$, et que $(\frac{1+b}{a})^4 = -1$. En déduire que n divise le nombre entier $N = A^4 + 1$, si $\bar{A} = \frac{1+b}{a}$.

Exercice 3.38 Montrer que 3 divise a et b si et seulement s'il divise $a^2 + b^2$.

Exercice 3.39 Montrer que l'équation : $x^2 - 16y - 11 = 0$ n'a pas de solution entière. (Réduire modulo 8).

3.3 Le 'petit' théorème de Fermat. Applications à la factorisation.

Théorème 3.40 Pour tous $a, b \in \mathbb{Z}$, si $n = p$ est premier, on a dans \mathbb{Z}_p : $(\bar{a} + \bar{b})^p = \bar{a}^p + \bar{b}^p$.

Démonstration : $(\bar{a} + \bar{b})^p = \sum_{k=0}^{k=p} \bar{C}_p^k \bar{a}^k \bar{b}^{p-k} = \bar{a}^p + \bar{b}^p$, puisque $\bar{C}_p^k = \bar{0}$ si $0 < k < p$, puisque C_p^k est alors divisible par p \square

Corollaire 3.41 ('Petit théorème de Fermat') Pour tout $a \in \mathbb{Z}$ et tout p premier, $a^p \equiv a[p]$. Si p ne divise pas a , alors $a^{p-1} \equiv 1[p]$.

Première démonstration : On peut supposer $a > 0$. L'assertion est vraie pour $a = 1$. On la déduit par récurrence sur a de 3.40, puisque : $\overline{(a+1)}^p = (\bar{a} + \bar{1})^p = \bar{a}^p + \bar{1}^p = \bar{a} + \bar{1} = \overline{a+1}$. (La troisième égalité n'est autre que l'hypothèse de récurrence).

Si p divise a , $a^{p-1} \equiv 0[p]$. Sinon, $(a, p) = 1$, donc il existe $u, v \in \mathbb{Z}$ tels que $u \cdot a + v \cdot p = 1$. Donc $u \cdot a \equiv 1[p]$. Donc $1 \equiv u \cdot a \equiv u \cdot a^p \equiv (u \cdot a) \cdot a^{p-1} \equiv a^{p-1}[p]$.

Seconde démonstration : Soit $\bar{P} := \bar{1} \cdot \bar{2} \cdot \dots \cdot \overline{p-1}$ le produit de toutes les classes non nulles de \mathbb{Z}_p . Alors les éléments $\bar{a}, \bar{2} \cdot \bar{a}, \bar{3} \cdot \bar{a}, \dots, \overline{p-1} \cdot \bar{a}$ forment une permutation des éléments $\bar{1}, \bar{2}, \dots, \overline{p-1}$, puisqu'ils sont deux-à-deux distincts (puisque $\bar{a} \cdot \bar{x} = \bar{a} \cdot \bar{y}$ implique $\bar{x} = \bar{y}$), et différents de $\bar{0}$. Leur produit est donc égal à \bar{P} , et aussi à $\bar{a}^{p-1} \cdot \bar{P}$. On en déduit que $\bar{a}^{p-1} = \bar{1}$, puisque $\bar{P} \neq \bar{0}$. \square

Remarque 3.42 *Ce corollaire est souvent utilisé pour montrer qu'un entier n n'est pas premier sans faire de division ni trouver l'un de ses facteurs. Il suffit, par exemple de montrer que 2^n n'est pas congru à 2 modulo n . Par exemple : $2^9 - 2 = 2 \cdot (2^8 - 1) = 2 \cdot (2^4 - 1)(2^4 + 1) = 2 \cdot 3 \cdot 5 \cdot 17 \equiv 6[9]$, et 9 n'est (évidemment) pas premier. Même lorsque n est très grand, on peut calculer a^n modulo n rapidement (en essentiellement $\log(n)$ opérations).*

Théorème 3.43 *Soit $a > 1$ entier, et p premier. Si q premier divise $a^p - 1$, alors $q \equiv 1[p]$, ou q divise $(a - 1)$. (Autrement dit : les diviseurs premiers de $a^p - 1$ sont soit ceux de $a - 1$, soit de la forme : $k \cdot p + 1$).*

Démonstration : $a^{q-1} \equiv [1][q]$ par le petit théorème de Fermat, et $a^p \equiv [1][q]$ par hypothèse. Soit $d := (p, q - 1)$. Puisque p est premier, deux cas seulement sont possibles : ou bien $d = p$ (et p divise donc $q - 1$), ou bien $d = 1$. Mais le lemme 3.44 ci-dessous montre qu'alors : $a^d = a \equiv [1][q]$, et q divise donc $(a - 1)$. \square

Lemme 3.44 *Soit $a > 1$ entier, $m > 0, n > 0, N > 1$ des entiers tels que : $a^m \equiv a^n \equiv [1][N]$. Alors $a^d \equiv [1][N]$ si $d := (m, n)$.*

Démonstration : Soit $u > 0, v > 0$ entiers tels que $u \cdot m - v \cdot n = d$ (quitte à échanger m et n). Alors $1 \equiv a^{um} = a^{vn} \cdot a^d \equiv a^d[N] \square$

Exemple 3.45 *Si $a = 2, q \equiv 1[p]$ si q premier divise $a^p - 1$ avec p premier, puisque $a - 1 = 2 - 1 = 1$ n'est pas divisible par q .*

Par exemple, tout diviseur premier de $N := 2^{11} - 1 = 2047$ est de la forme $k \cdot 22 + 1$, puisque impair. Le plus petit diviseur premier est au plus $\sqrt{2^{11}} = 2^5 \cdot \sqrt{2} < 45$. Les nombres premiers de la forme $22 \cdot k + 1$ sont : 23, 67, 89, ... Le seul diviseur premier possible de N est donc 23 si N n'est pas premier. Une division montre que $2047 = 2300 - 230 - 23 = 23 \cdot (100 - 10 - 1) = 23 \cdot 89$.

Corollaire 3.46 *Soit q un nombre premier impair. Il existe une infinité de nombres premiers $p \equiv 1[2q]$.*

Démonstration : Il suffit de montrer que si $p_1 < p_2 < \dots < p_r$ sont des nombres premiers congrus à 1 modulo q , il est possible de construire p premier tel que $p \equiv 1[q]$ et $p \neq p_j, j = 1, \dots, r$. Soit $P := p_1 \cdot \dots \cdot p_r, a := q \cdot P$, et $N := a^{q-1} + a^{q-2} + \dots + a + 1$. Soit maintenant p premier diviseur de N . Alors p divise $N \cdot (a - 1) = a^q - 1$, mais ne divise pas $(a - 1)$, puisque l'on aurait alors : $a \equiv [1][p]$, et donc $N \equiv [1][p]$, donc $p = q$ divise $qP - 1$, ce qui est impossible. D'après 3.43, $p \equiv 1[q]$. Puisque p est premier avec $a = q \cdot P$, il est premier avec, donc différent de, chacun des p_j . \square

Remarque 3.47 *Le 'théorème de la progression arithmétique' de Dirichlet affirme, plus généralement, l'existence d'une infinité de nombres premiers $p \equiv b[a]$ pour tout couple entiers a, b premiers entre eux. Ses démonstrations reposent toutes sur l'analyse. Nous allons démontrer un autre cas particulier : $a = 8, b = 5$, ou 1.*

Corollaire 3.48 Soit $N = a^2 + b^2$ un nombre impair somme de deux carrés d'entiers, et p un diviseur premier (donc impair) de N . Alors $p \equiv 1[4]$ si p ne divise pas b .

Démonstration : L'un des deux nombres a ou b exactement est impair. Supposons que ce soit b .

On suppose tout d'abord que $b^2 \equiv 1[p]$. Alors $a^2 \equiv -1[p]$. Par le petit théorème de Fermat, on a donc : $1 \equiv a^{p-1} = (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}[p]$, donc $\frac{p-1}{2}$ est pair, et $p \equiv 1[4]$. Un second argument, plus long mais généralisable (voir 3.50), est le suivant : p divise $(a^4 - 1)$ et $(a^{p-1} - 1)$, donc $(a^d - 1)$ si $d = (p-1, 4)$, d'après 3.44. Donc $d = 1, 2$ ou 4 . Mais d ne peut être 1 ou 2 , puisque $a^2 \equiv -1[p]$. Donc 4 divise $(p-1)$.

Dans le cas général, il existe par Bezout, puisque p ne divise pas b , un entier u tel que $ub \equiv 1[p]$. On remplace a, b par $A := ua$ et $B := ub$, et on est ramenés au cas précédent. \square

Corollaire 3.49 Il existe une infinité de nombres premiers $p \equiv 5[8]$ (et donc aussi congrus à 1 modulo 4).

Démonstration : Soit P le produit d'un ensemble fini de tels nombres premiers (tous impairs). Soit $N := P^2 + 2^2$. Le corollaire précédent montre que tous les diviseurs premiers de N sont congrus à 1 modulo 4 , donc congrus à 1 ou 5 modulo 8 , et premiers à P . Si tous ces diviseurs premiers étaient congrus à 1 modulo 8 , N le serait aussi, or $N \equiv 5[8]$, puisque le carré de tout nombre impair est congru à 1 modulo 8 . \square

Nous allons généraliser 3.48 ci-dessus, en y remplaçant l'exposant 2 par 2^k .

Corollaire 3.50 Soit $a, b, k > 0$ entiers, $N = a^{2^k} + b^{2^k}$, et p un diviseur premier impair de N . Alors $p \equiv 1[2^{k+1}]$ si p ne divise pas b .

Démonstration : C'est essentiellement la même avec le second argument) que pour $k = 1$, et on peut supposer que $b = 1$ par le même argument. Dans ce cas : $a^{2^k} \equiv -1[p]$, donc p divise $(a^{2^{k+1}} - 1)$ et $(a^{p-1} - 1)$, donc aussi $(a^d - 1)$ si $d = (p-1, 2^{k+1})$, d'après 3.44. Puisque d divise 2^{k+1} , $d = 2^\ell$, avec $0 \leq \ell \leq (k+1)$. Mais puisque $a^{2^k} \equiv -1[p]$, on a : $\ell = k+1$, et 2^{k+1} divise donc $(p-1)$. \square

Remarque 3.51 L'exposant $(k+1)$ est optimal ($a = 3, b = 1, k = 2$) en général, mais pas lorsque $a = 2, b = 1$, auquel cas on a toujours $p \equiv 1[2^{k+2}]$.

On déduit de 3.50 comme en 3.49 ci-dessus en considérant $N = (2P)^{2^k} + 1$ le :

Corollaire 3.52 Soit $k \geq 1$ entier. Il existe une infinité de nombres premiers congrus à 1 modulo 2^k .

Remarque 3.53 En considérant les polynômes 'cyclotomiques' on peut généraliser le résultat précédent aux nombres premiers congrus à 1 modulo n , pour tout $n > 1$. Lorsque $n = p^r$, p premier, on peut procéder directement comme en 3.50 ci-dessus (où nous avons traité le cas $p = 2$).

3.4 Exercices.

40 Soit p un nombre premier tel que $q := 2p + 1$ soit aussi premier. (Ex : $p = 2, 3, 5, 11$). Si l'équation $a^p + b^p = c^p$ a une solution entière a, b, c , alors abc est divisible par q . Vérifier pour $p = 2, q = 5$.

Exercice 3.54 Décomposer $2^{13} - 1$ en produit de facteurs premiers.

Exercice 3.55 Si $p \neq q$ sont premiers, si $b > 0, k \geq 0$ sont entiers, et si on pose : $a = b^{p^k}$ et $N := a^{p-1} + a^{p-2} + \dots + a^2 + a + 1$, montrer que si q divise N , alors $q \equiv 1[p^{k+1}]$.

Exercice 3.56 Montrer, pour tout p premier et tout $k > 0$, l'existence d'une infinité de nombres premiers q tels que $q \equiv 1[p^{k+1}]$.

Exercice 3.57 Montrer que si q premier divise le nombre de Fermat $F_k := 2^{2^k} + 1$, alors $q \equiv 1[2^{k+1}]$. (On montrera dans l'exercice qui suit que, en fait, on a même : $q \equiv 1[2^{k+2}]$).

Utilisant ce dernier résultat, montrer (presque) sans calculs que $F_3 = 2^8 + 1 = 257$ et $F_4 = 2^{16} + 1 = 65.537$ sont premiers.

Exercice 3.58 Soit $F_n = 2^{2^n} + 1, n \geq 2$ le n -ième nombre de Fermat, et p un diviseur premier de F_n .

1. Soit $a := 2^{2^{n-2}}$. Montrer que $a^4 \equiv -1[p]$.
2. Soit $b := \bar{a} + \bar{a}^{-1} \in \mathbb{Z}_p, \bar{a}^{-1}$ y étant l'inverse de \bar{a} . Montrer que $b^2 = \bar{2} \in \mathbb{Z}_p$.
3. Montrer que $b^{2^{2^{n+1}}} \equiv -1[p]$.
4. En déduire que $(p - 1, 2^{n+2}) = 2^{n+2}$, et que $p \equiv 1[2^{n+2}]$.
5. Montrer que tout diviseur premier de F_5 est de la forme $1 + 128.k, k$ entier, et que le plus petit nombre premier de cette forme (hormis $F_3 = 257$, premier avec F_5) est 641.

Exercice 3.59 Soit $F_n := 2^{2^n} + 1, n \geq 0$ entier le n -ième nombre de Fermat. On pose : $A := 3^{\frac{F_n-1}{2}}$, et on se propose de montrer que F_n est premier si et seulement si $A \equiv -1[F_n]$.

1. Montrer soigneusement que si F_n est premier, alors $A^2 \equiv 1[F_n]$. En déduire que $A \equiv \pm 1[F_n]$, et enfin que $A \equiv -1[F_n]$.

2. Si $A \equiv -1[F_n]$, et si q est un diviseur premier de $A^2 - 1$, montrer que $3^{F_n-1} \equiv 3^{q-1} \equiv 1[q]$. En déduire que $3^d \equiv 1[q]$, si d est le PGCD de $(q - 1)$ et de $(F_n - 1)$. En déduire que $q = 2^s$, pour un entier $0 \leq s \leq 2^{n-1}$, puis que $q = F_n$.

3. Peut-on remplacer 3 par d'autres nombres entiers $m > 0$ dans la définition de A ci-dessus, de telle sorte que F_n soit premier si et seulement si $m^{\frac{F_n-1}{2}} \equiv -1[F_n]$? Si oui, par lesquels, et pourquoi ?

Exercice 3.60 Soient m', n' des entiers strictement positifs premiers entre eux.

1. Si $d > 0$ est entier, montrer qu'il existe des entiers strictement positifs μ, ν, δ uniques tels que : $d = \mu.\nu.\delta$, et : $1 = (\mu, n') = (\nu, m') = (\mu, \nu) = (\mu, \nu, \delta) = (m'.n', \delta)$

2. Si m et n sont des entiers strictement positifs, montrer l'existence d'entiers a et b tels que : $a|m$, $b|n$, $(\frac{m}{a}, \frac{n}{b}) = 1$, et : $\frac{m}{a} \cdot \frac{n}{b} = m \cap n$. (Observer que $a \cdot b = (m, n) := d$, et que $(\frac{m}{d}, \frac{n}{d}) = 1$).

3.5 *Nombres pseudopremiers.

Théorème 3.61 Soit $n > 2$ un entier impair. S'il existe $a \in \mathbb{Z}$ premier avec n et tel que a^{n-1} ne soit pas congru à 1 modulo n , alors n est "composé" (ie : n'est pas premier. La démonstration ne fournit cependant aucun facteur non-trivial de n).

Démonstration : Par Fermat, $a^{n-1} \equiv 1[n]$ si n était premier \square

Exemple 3.62 $n = 105 (= 3 \cdot 5 \cdot 7)$ n'est pas premier, puisque $2^{104} = (2^6)^{17} \times 2^2 \equiv 4[7]$, de sorte que 2^{104} n'est pas congru à 1 modulo 105.

Théorème 3.63 Soit $n > 2$ un entier impair. Alors n est premier s'il existe $a \in \mathbb{Z}$ premier avec n et tel que :

1. $a^{n-1} \equiv 1[n]$.
2. $a^{\frac{n-1}{q}}$ ne soit congru à 1 modulo n , pour aucun des nombres premiers q divisant $(n-1)$.

Démonstration : Soit $r > 0$ le plus petit des entiers $m > 0$ tels que $a^m \equiv 1[n]$. Donc r divise $(n-1)$, par 1. Si $r \neq (n-1)$, r divise l'un des $\frac{(n-1)}{q}$, ce qui est impossible par 2. Donc $r = (n-1)$, et es $(n-1)$ nombres a^k , pour $k = 1, \dots, (n-1)$ sont tous différents (modulo n), et premiers avec n . Donc n est premier. \square

On affinera le test de primalité précédent dans la section ??.

Definition 3.64 On dit que n , impair et non premier, est pseudopremier en base $b \in \mathbb{Z}$ si $b^{n-1} \equiv 1[n]$. En particulier, $b, n) = 1$.

On dit que n , impair et non premier, est pseudopremier (ou de Carmichael) si $b^{n-1} \equiv 1[n]$ pour tout $b \in \mathbb{Z}$ tel que $(b, n) = 1$.

Exemple 3.65

1. $n = 105 (= 3 \cdot 5 \cdot 7)$ est pseudo-premier en base 13, mais pas en base 2. En effet : $13^{104} \equiv 1$ modulo 3, 5, 7. Mais $2^{104} = (2^6)^{17} \times 2^2 \equiv 4[7]$.

2. $n = 91$ est pseudopremier en base 3, mais pas en base 2.

3. $n = 561 = 3 \cdot 11 \cdot 17$ est pseudopremier, puisque $\lambda(561) = \text{ppcm}(2, 12, 16) = 48$ divise $560 = 7 \cdot 8 \cdot 10 = 16 \cdot 5 \cdot 7$.

Proposition 3.66 Si n est pseudo premier, il est sans facteur carré (i.e : il n'est divisible par aucun carré de nombre premier).

Démonstration : Si p^2 divise n , p divise $(n-1)$, par le lemme 3.67 ci-dessous (puisque $a^d \equiv 1[n]$, si $d = (p, (n-1)) = 1$ ou p). Or $(n-1)$ (est donc p) est premier avec n . Contradiction. \square

Lemme 3.67 Si p est premier, et si p^2 divise n , il existe a premier avec n tel que $a^p \equiv 1[n]$, mais tel que a ne soit pas congru à 1 modulo n .

Démonstration : Posons $n = n'.p^s$, avec $s \geq 2$, et $(n', p) = 1$. Il suffit de choisir $a = 1 + n'.p^{s-1}$. \square

Remarque 3.68 Il a été démontré en 1992 (seulement) qu'il y a une infinité de nombres pseudopremiers.

3.6 Exercices

Exercice 3.69 Factoriser $3^{12} - 1 = 531440$.

Exercice 3.70 Sachant que $n = 122921$ divise $N := 2^{35} - 1$, montrer que n est premier.

Exercice 3.71 Factoriser $N := 2^{35} - 1 = 34359738367$. (On pourra utiliser : $\frac{N}{31.127} = 8727391$, et le fait que les nombres premiers congrus à 1 modulo 70 sont : 71, 211, 281, ...). (La factorisation est : $N = 31.71.127.122921$).

Exercice 3.72 Soit $n \geq 3$ un entier impair. Montrer que $2^n + 1$ est divisible par 3, et que si $\frac{2^p+1}{3}$ est premier, alors n est premier.

Factoriser $N := \frac{2^p+1}{3}$ si $p = 3, 5, 7, 11, 13, 19$ après avoir montré que $2p$ divise $q - 1$, pour chacun des facteurs premiers de N .

Exercice 3.73 Soit $n := 2^{24} + 1 = 16777217$.

1. Trouver un nombre de Fermat qui divise n .
2. Montrer que tout autre diviseur premier de n est congru à 1 modulo 48.
3. Factoriser n .

Exercice 3.74 Factoriser les nombres n suivants : $3^{15} - 1, 3^{24} - 1, 5^{12} - 1, 10^5 - 1, 10^6 - 1, 10^8 - 1, 2^{33} - 1, 2^{21} - 1, 2^{15} - 1, 2^{30} - 1, 2^{60} - 1$

Exercice 3.75 Soit $m > 0$ un entier tel que $6m + 1, 12m + 1$ et $18m + 1$ soient premiers. Donner un exemple de tel m (on ne sait pas s'il en existe une infinité). Montrer que $N := (6m + 1).(12m + 1).(18m + 1)$ est pseudopremier.

Exercice 3.76 Montrer que les nombres suivants sont pseudopremiers :

$$1105, 1729, 2465, 2821, 6601 = 7.23.41, 29341 = 13.37.61, 172081 = 7.13.31.61, \\ 278545 = 5.17.29.113.$$

Exercice 3.77 Trouver toutes les bases b pour lesquels 15, 21, 91 sont pseudopremiers. Indication : pour tout diviseur premier p de n , l'ordre multiplicatif de b modulo p doit diviser $(p - 1)$ et $(n - 1)$.

Montrer que si p et $2p - 1$ sont premiers, $n := p.(2p - 1)$ est pseudopremier relativement à exactement la moitié des bases $b \in \mathbb{Z}_n^*$: celles qui sont des carrés modulo $(2p - 1)$.

Exercice 3.78 * Soit n impair composé (ie : non premier), p premier, et $b \in \mathbb{Z}_n^*$.

1. Montrer que si p divise n et si $n' := n/p$, alors n est pseudopremier en base b si et seulement si $b^{n'-1} \equiv 1[p]$.

2. En déduire que $n = 3.p, p > 3$ n'est pas pseudopremier en bases $b = 2, 5, 7$.

3. En déduire que $n = 5.p, p > 5$ n'est pas pseudopremier en bases $b = 2, 3, 7$.

4. Montrer que 91 est le plus petit nombre pseudopremier en base 3.

5. Déterminer les plus petits nombres pseudopremiers en bases 2 ou 5.

Exercice 3.79 Montrer que $n = p^2$, p premier impair, est pseudo premier en base b si et seulement si $b^{p-1} \equiv 1[p^2]$. Indication : comparer $(n-1)$ et $\varphi(n)$.

Exercice 3.80 * Soit $n = p.q$ le produit de deux nombres premiers distincts. Soit $d = (p-1, q-1)$.

1. Montrer que n est pseudopremier en base b si et seulement si $b^d \equiv 1[n]$.

2. Déterminer le nombre B_n de bases $b \in \mathbb{Z}_n$ en lesquelles n est pseudopremier en fonction de d .

3. Cas particulier où $q = 2p + 1$. Les décrire en fonction de p .

3. Si $n = 341$, quelle est la proportion $B_{341}/\varphi(n)$ de ces bases ?

Exercice 3.81 * Si n est pseudopremier en base 2, montrer que $2^n - 1$ l'est aussi.

Montrer que si n est pseudopremier en base b , et si $(b-1, n) = 1$, alors $N := \frac{b^n - 1}{b-1}$ l'est aussi. Montrer qu'on ne peut omettre la condition $(b-1, n) = 1$.

Montrer qu'il existe une infinité de nombres pseudopremiers en base b pour $b = 2, 3, 5$

Exercice 3.82 * Soit $b > 1$ un entier, et p premier ne divisant pas $b, b-1, b+1$. Soit $n := \frac{b^{2p}-1}{b^2-1}$. Montrer que :

1. n est composé, et que $2p \mid (n-1)$.

2. n est pseudopremier en base b , et qu'il existe une infinité de nombres pseudopremiers en base b .

Exercice 3.83 * Déterminer tous les nombres pseudopremiers de la forme : $3.p.q$ ou $5.p.q$, avec $p < q$ premiers. (Utiliser l'exercice 3.78(1)).

Montrer que, pour tout nombre premier r fixé, les nombres premiers $p < q$ tels que $n := r.p.q$ soit pseudopremier sont en nombre fini.

Exercice 3.84 * Montrer que $561 = 3.11.17$ est le plus petit nombre pseudopremier.

3.7 *Théorème d'Euler. Symbole de Legendre.

On a aussi le raffinement important suivant du théorème de Fermat :

Théorème 3.85 (Euler) Soit p premier impair, et $\bar{a} \in \mathbb{Z}$. Alors $\bar{a}^{\frac{p-1}{2}} = \pm \bar{1} \in \mathbb{Z}_p$.

Démonstration : Soit $b := a^{\frac{p-1}{2}} \in \mathbb{Z}$. Alors $b^2 \equiv 1[p]$ par Fermat. Donc p divise $b^2 - 1 = (b-1)(b+1)$. Donc p divise l'un des deux facteurs, puisque p est premier. \square

Definition 3.86 On note : $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) = \pm 1[p]$, et on l'appelle le symbole de Legendre (de a modulo p).

Definition 3.87 On dit que $\bar{a} \in \mathbb{Z}_n, n > 1$ est un carré de \mathbb{Z}_n s'il existe $\bar{c} \in \mathbb{Z}_n$ tel que $\bar{c}^2 = \bar{a} \in \mathbb{Z}_n$.

Proposition 3.88 Soit $\bar{a}, \bar{b} \in \mathbb{Z}_p, p$ premier. Alors :

1. $\left(\frac{\bar{a}\bar{b}}{p}\right) = \left(\frac{\bar{a}}{p}\right) \cdot \left(\frac{\bar{b}}{p}\right)$.
2. Si $\bar{a} \in \mathbb{Z}_p$ est un carré de \mathbb{Z}_p , alors $\left(\frac{\bar{a}}{p}\right) = +1$.

Remarque 3.89 1. La réciproque de 3.88.2 est vraie (on le verra ci-dessous dans la section "résidus quadratiques"). Donc a n'est pas un carré de \mathbb{Z}_p si $\left(\frac{a}{p}\right) = -1$. Par exemple : si $p \equiv 3[4]$, alors $\left(\frac{-1}{p}\right) = -1$, et -1 n'est pas un carré modulo p . Il l'est par contre dans l'autre cas possible : $p \equiv 1[4]$.

2. On définit, si $n = p_1 \dots p_s$ est un produit de nombres premiers impairs (pas forcément distincts) le symbole de Jacobi $\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_s}\right) = \pm 1$. Voir exercice ?? pour ses propriétés.

3.8 Exercices.

Exercice 3.90 On identifie $a \in \mathbb{Z}$ et sa classe $\bar{a} \in \mathbb{Z}_p$. Si p premier, divise $N = a^4 + 1$, a entier, montrer que :

1. $p \equiv 1[8]$, et $a \in \mathbb{Z}_p$.
3. Déterminer les deux plus petits nombres premiers p tels que $p \equiv 1[8]$.
2. Si $b := a + a^{-1}$ dans \mathbb{Z}_p^* , alors $b^2 = 2 \in \mathbb{Z}_p$.
3. Trouver b tel que $b^2 = 2$ dans \mathbb{Z}_p , si $p = 17, 41, 257, 313$

Exercice 3.91 Soit $a \in \mathbb{Z}$, et $p \neq 3$ un diviseur premier de $N := a^2 + a + 1$.

1. Montrer que $p \equiv 1[6]$.
2. Soit $b := 2a + 1$. Montrer que $b^2 \equiv -3[p]$.
3. Montrer que les conclusions (préciser) subsistent si N et b sont remplacés respectivement par $N' := a^2 - a + 1$ et $b' := 2a - 1$.
4. Trouver $c \in \mathbb{Z}$ tel que $c^2 \equiv -3[p]$ si $p = 37, 13, 19, 73$ (considérer $a = 10, 8$).
5. Trouver $d \in \mathbb{Z}$ tel que $d^2 \equiv 3[p]$ si $p = 37, 13, 73$. (Écrire p comme somme de deux carrés d'entiers).
6. Existe-t-il $d \in \mathbb{Z}$ tel que $d^2 \equiv 3[19]$? Justifier.

Exercice 3.92 Soit $a \in \mathbb{Z}$, et $p \neq 5$ un diviseur premier de $N := a^4 + a^3 + a^2 + a + 1$.

1. Montrer que $p \equiv 1[10]$.
2. Soit $b := a^4 + a - (a^2 + a^3)$. Calculer $(b - 1)$ et $(b + 1)$ modulo p en utilisant le fait que $(a^4 + a^3 + a^2 + a) \equiv -1[p]$.
3. En déduire que $b^2 \equiv 5[p]$. (Calculer $b^2 - 1$ en utilisant la question précédente).
4. Trouver $c \in \mathbb{Z}$ tel que $c^2 \equiv 5[p]$ si $p = 31$ et $p = 71$ (considérer $a = 2$ et $a = 5$).

Exercice 3.93 Montrer qu'il n'existe pas d'identité $(x^2 + y^2 + z^2)(X^2 + Y^2 + Z^2) = A^2 + B^2 + C^2$, avec A, B, C combinaisons linéaires à coefficients entiers en x, y, z, X, Y, Z . (Indication : $15 = 3 \cdot 5 = 8 + 7$). Remarquer qu'il existe, par contre, de telles identités avec des sommes de 2 et 4 carrés. Pour 2 carrés, on a : $(x^2 + y^2)(X^2 + Y^2) = (xX - yY)^2 + (xY + yX)^2$, par la multiplicativité du module des nombres complexes, pour 4 carrés on a une identité similaire déduite de la multiplicativité de la norme des quaternions.

Exercice 3.94 Vérifier que $(a^2 + b^2 + c^2 + d^2) \cdot (A^2 + B^2 + C^2 + D^2) = u^2 + v^2 + w^2 + t^2$, pour tous nombres complexes a, b, c, d, A, B, C, D , si : $u = aA + bB + cC + dD$, $v = aB - Ab + dC - Dc$, $w = aC - Ca + bD - Bd$, $t = aD - Ad + cB - Cb$.

Ecrire $15 = 3 \cdot 5$ et $161 = 7 \cdot 23$ comme somme de 4 carrés à l'aide de cette formule.

Exercice 3.95 Ecrire 161 comme somme de 4 carrés à l'aide de la formule 3.94.

3.9 *Théorème de Wilson.

Théorème 3.96 Soit $n \geq 3$ entier. Alors n est premier si et seulement si $(n-1)! \equiv -1[n]$.

Démonstration : Si $1 < a < n$ est un diviseur strict de n , alors a divise $(n-1)!$ Si $(n-1)! \equiv -1[n]$, on a aussi $0 \equiv (n-1)! \equiv -1[a]$. Contradiction. Donc n est premier si $(n-1)! \equiv -1[n]$. Supposons maintenant que n est premier impair. Remarquons que $X^2 = \bar{1} a$, dans \mathbb{Z}_n^* , seulement les solutions $\bar{a} = 1$ et $\bar{a} = -\bar{1}$, puisque $X^2 - 1 = (X - \bar{1})(X + \bar{1})$, et qu'un produit de deux facteurs non nuls de \mathbb{Z}_n , n premier, est non nul. Modulo n , si $a^2 \neq 1$, l'inverse a' de a est donc différent de a , si a diffère de $\bar{1}$ et de $-\bar{1}$. Les $n-1$ éléments de \mathbb{Z}_n^* se répartissent donc en $(n-3)$ couples d'éléments a, a' dont le produit est $\bar{1}$, et le couple : $\bar{1}, -\bar{1}$ dont le produit est $-\bar{1}$, qui est donc égal au produit de tous les éléments de \mathbb{Z}_n \square

Exemple 3.97 Soit p un nombre premier impair. Posons : $r = \frac{p-1}{2}$. Alors : soit $p \equiv 1[4]$, et r est pair, soit $p \equiv -1 = 3[4]$ et r est impair. Dans le second cas, -1 n'est pas le carré a^2 d'un élément a de \mathbb{Z}_p (sinon : $-1 = (-1)^{\frac{p-1}{2}} = (a^2)^{\frac{p-1}{2}} = a^{(p-1)} = +1$, par Fermat). Dans le premier cas, $(r!)^2 \equiv -1[p]$. En effet : pour tout $1 \leq a \leq r$, $(\frac{p+1}{2}) \leq p-a \leq (p-1)$. Comme il y a r tels facteurs, on a : $-1 \equiv (p-1)! \equiv r!(-1)^r r! = (-1)^r \cdot (r!)^2 = (r!)^2[p]$

Prenons $p = 13 \equiv 1[4]$. Alors $r = 6$ et $6! = 720 \equiv 5[13]$. On vérifie en effet que : $5^2 = 25 = 26 - 1 \equiv -1[13]$.

3.10 Exercices

Exercice 3.98 Montrer que $t(n) := \frac{1}{1 + \sum_{k=2}^{n-1} \left(\binom{n}{k} - \binom{n-1}{k} \right)}$ vaut 1 si n est premier et 0 sinon.

Exercice 3.99 Montrer que $T(n) := \left[\frac{(n-1)!+1}{n} \right] - \left[\frac{(n-1)!}{n} \right]$ vaut aussi 1 si n est premier et 0 sinon.

Exercice 3.100

4 ÉLÉMENTS INVERSIBLES DE \mathbb{Z}_n^* .

4.1 Éléments inversibles de \mathbb{Z}_n .

Soit $n > 0$ un entier, et \mathbb{Z}_n l'ensemble des classes d'entiers modulo n muni de ses deux opérations $+$ et \times . On note \bar{a} la classe dans \mathbb{Z}_n d'un entier $a \in \mathbb{Z}$.

Definition 4.1 On dit que \bar{a} est inversible (dans \mathbb{Z}_n) s'il existe \bar{b} in \mathbb{Z}_n tel que $\bar{a}.\bar{b} = \bar{1}$. On note \mathbb{Z}_n^* l'ensemble des éléments inversibles de \mathbb{Z}_n (qui est toujours non vide, puisque $\bar{1} \in \mathbb{Z}_n$). On note aussi $\varphi(n)$ le cardinal de \mathbb{Z}_n^* . La fonction $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ ainsi définie est appelée 'indicatrice' d'Euler.

Proposition 4.2 Supposons que \bar{a} et \bar{a}' soient dans \mathbb{Z}_n^* , et \bar{c}, \bar{d} dans \mathbb{Z}_n . Alors :

1. Il existe un unique $\bar{b} \in \mathbb{Z}_n$ tel que $\bar{a}.\bar{b} = \bar{1}$. On l'appelle 'inverse' de \bar{a} (dans \mathbb{Z}_n), et on le note \bar{a}^{-1} .
2. \bar{a}^{-1} est inversible, d'inverse \bar{a} .
3. $\bar{a}.\bar{a}'$ est inversible, son inverse est $\bar{a}^{-1}.\bar{a}'^{-1}$.
4. Si $\bar{a}.\bar{c} = \bar{a}.\bar{d}$, alors $\bar{c} = \bar{d}$. En particulier, $\bar{a}.\bar{c} \neq \bar{0}$ si $\bar{c} \neq \bar{0}$.

Proposition 4.3 Soit $\bar{a} \in \mathbb{Z}_n$. Alors on a équivalence entre les deux propriétés suivantes :

1. $\bar{a} \in \mathbb{Z}_n^*$.
2. $(a, n) = 1$, pour tout $a \in \mathbb{Z}$ dont la classe est \bar{a} .

Démonstration : Si $\bar{a}.\bar{b} = \bar{1}$, alors $\overline{a.b} = \bar{1}$, donc $a.b - 1 = k.n$ pour un $k \in \mathbb{Z}$. Donc $a.b - k.n = 1$, et $(a, n) = 1$. Réciproquement, si $(a, n) = 1$, il existe b et k tels que $a.b - k.n = 1$, et donc $\bar{a}.\bar{b} = \bar{1}$. \square

On va maintenant calculer $\varphi(n)$ en fonction de la décomposition en facteurs premiers de n .

4.2 exercices

Exercice 4.4 Déterminer (après avoir établi son existence) l'inverse de \bar{a} dans \bar{n} lorsque $(a, n) = (4, 17), (5, 17), (7, 71), (23, 71)$.

Exercice 4.5

Exercice 4.6

Exercice 4.7

Exercice 4.8

Exercice 4.9

4.3 Théorème Chinois.

Il permet de ramener l'étude de \mathbb{Z}_N pour N arbitraire au cas, beaucoup plus simple, où N est une puissance de nombre premier.

Théorème 4.10 *Soit $a > 0$, et $b > 0$ deux entiers premiers entre eux. Pour tous couples d'entiers α, β , il existe un entier n tel que $n \equiv \alpha[a]$, et $n \equiv \beta[b]$. De plus, n est unique modulo ab .*

Démonstration : Existence. Résolvons d'abord les cas : $(\alpha, \beta) = (1, 0)$ et $(\alpha, \beta) = (0, 1)$. L'algorithme de Bezout fournit une égalité $ua + bv = 1$. Le choix de $n_1 = bv$ (resp. $n_2 = ua$) fournit une solution à $n_1 \equiv 1[a]$, et $n_1 \equiv 0[b]$ (resp. à $n_2 \equiv 0[a]$, et $n_2 \equiv 1[b]$). Le choix de $n := \alpha.n_1 + \beta.n_2$ fournit une solution au problème initial.

Unicité. Si n et n' sont deux solutions, $n - n'$ est divisible par a et par b , donc par ab , puisque $(a, b) = 1$. \square

Exemple 4.11 *Si $a = 19, b = 31, \alpha = 3, \beta = 5$, alors $31 = 19 + 12, 19 = 12 + 7, 12 = 7 + 5, 7 = 5 + 2, 5 = 2 + 1$. Donc $1 = -2.2 + 5 = -2.(7 - 5) + 5 = 3.5 - 2.7 = 3.(12 - 7) - 2.7 = 3.12 - 5.7 = 3.12 - 5.(19 - 12) = 8.12 - 5.19 = 8.(31 - 19) - 5.19 = 8.31 - 13.19$. Donc $n = 3.8.31 - 5.13.19$ est congru à 3 modulo 19 et à 5 modulo 31.*

Corollaire 4.12 *Si a_1, \dots, a_k sont des entiers positifs premiers entre eux deux à deux, et si $\alpha_1, \dots, \alpha_k \in \mathbb{Z}$, il existe un entier n tel que $n \equiv \alpha_j[a_j], \forall j = 1, \dots, k$. L'entier n est unique modulo $a_1 \dots a_k$.*

Démonstration : Récurrence sur $k \geq 2$, à l'aide de 4.10. \square

Exemple 4.13 *$k = 3, a_j = 19, 31, 17, \alpha_j = 3, 5, 7$ pour $j = 1, 2, 3$ respectivement.*

Proposition 4.14 *Soit n, N des entiers positifs. Si n divise N , il existe une unique application $g := p_{n,N} : \mathbb{Z}_N \rightarrow \mathbb{Z}_n$ telle que, pour tout $a \in \mathbb{Z}$, on ait :*

1. $p_{n,N}(\bar{a}^N) = p_{n,N}(\bar{a}^n)$.
- On a , de plus, pour tous $a, b \in \mathbb{Z}$:
2. $g(\bar{a}^N + \bar{b}^N) = \bar{a}^n + \bar{b}^n$.
3. $g(\bar{a}^N \cdot \bar{b}^N) = \bar{a}^n \cdot \bar{b}^n$.

Démonstration : 1. Il suffit de montrer que, pour tous $a, a' \in \mathbb{Z}$, si $a \equiv a'[N]$, alors $a \equiv a'[n]$, ce qui est évident, puisque $n|N$.

2. Par définition, $g(\bar{a}^N + \bar{b}^N) = g(\overline{a + b}^N) = \overline{a + b}^n := \bar{a}^n + \bar{b}^n$.
3. Par définition, $g(\bar{a}^N \cdot \bar{b}^N) = g(\overline{a \cdot b}^N) = \overline{a \cdot b}^n := \bar{a}^n \cdot \bar{b}^n$. \square

Corollaire 4.15 *Soit m, n deux entiers strictement positifs, avec $N = m.n$. On a donc une application produit $f : \mathbb{Z}_{m.n} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ définie par : $f(\bar{a}^{m.n}) := (\bar{a}^m, \bar{a}^n)$, pour tout $a \in \mathbb{Z}$.*

1. Si $(m, n) = 1$, alors f est bijective.

Si $f^{-1} : \mathbb{Z}_m \times \mathbb{Z}_n \rightarrow \mathbb{Z}_{m.n}$ est son application réciproque, alors pour tous $a, a', b, b' \in \mathbb{Z}$, on a :

2. $f^{-1}(\bar{a}^n + \bar{a}'^n, \bar{b}^n + \bar{b}'^n) = f^{-1}(\bar{a}^n, \bar{b}^n) + f^{-1}(\bar{a}'^n, \bar{b}'^n)$.
3. $f^{-1}(\bar{a}^n \cdot \bar{a}'^n, \bar{b}^n \cdot \bar{b}'^n) = f^{-1}(\bar{a}^n, \bar{b}^n) \cdot f^{-1}(\bar{a}'^n, \bar{b}'^n)$

Démonstration : 1. C'est une reformulation de 4.10.

2. On applique f aux deux membres. Par injectivité de f , il suffit de voir que $(\bar{a}^n + \bar{a}'^n, \bar{b}^n + \bar{b}'^n) = f(u^N + v^N)$, si $f(u) = (\bar{a}^n, \bar{b}^n)$, et $f(v) = (\bar{a}'^n, \bar{b}'^n)$. Mais $f(\bar{u}^N + \bar{v}^N) = f(\overline{u + v^N}) = (\overline{u + v^m}, \overline{u + v^n}) = (\bar{u}^m + \bar{v}^m, \bar{u}^n + \bar{v}^n) = (\bar{a}^n + \bar{a}'^n, \bar{b}^n + \bar{b}'^n)$.

3. Même démonstration en y remplaçant l'addition par la multiplication. \square

Une récurrence sur $s \geq 1$ montre alors le :

Corollaire 4.16 Si $N = p_1^{r_1} \dots p_s^{r_s}$ est la décomposition de N en produit de facteurs premiers, on pose $N_j := p_j^{r_j}$ pour $j = 1, \dots, s$. Alors l'application naturelle : $G : \mathbb{Z}_N \rightarrow \mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_s^{r_s}}$ définie par $G(\bar{a}^N) = (\bar{a}^{N_1}, \dots, \bar{a}^{N_s})$ est une bijection compatible avec l'addition et la multiplication terme-à-terme des facteurs (comme dans le corollaire précédent).

4.4 Exercices.

4.5 Indicatrice d'Euler.

Soit $n > 0$. On va calculer $\varphi(n)$. La propriété cruciale est la suivante :

Théorème 4.17 Soit $m > 0$ et $n > 0$ entiers. Si $(m, n) = 1$, alors $\varphi(m.n) = \varphi(m) \cdot \varphi(n)$.

Démonstration : Posons $N := m.n$. Soit $G : \mathbb{Z}_N \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ l'application définie par $G(\bar{a}^N) = (\bar{a}^m, \bar{a}^n)$. Rappelons qu'elle est bijective. On va montrer que $G(\mathbb{Z}_N^*) = \mathbb{Z}_m^* \times \mathbb{Z}_n^*$, ce qui établira le résultat, puisqu'alors G est une bijection entre \mathbb{Z}_N^* et son image, et que par définition : $\varphi(N), \varphi(m), \varphi(n)$ sont les cardinaux de $\mathbb{Z}_N^*, \mathbb{Z}_m^*, \mathbb{Z}_n^*$ respectivement. Soit donc $a \in \mathbb{Z}$ tel que $(a, m.n) = 1$, on a donc aussi : $(a, m) = (a, n) = 1$, puisque ces nombres divisent $(a, m.n)$. \square

Remarque 4.18 L'application G ayant pour bijection réciproque $G^{-1}(\bar{\alpha}, \bar{\beta}) := \overline{vn\alpha + um\beta}^{mn}$ si $um + nv = 1$ et si $\bar{\alpha}^m \in \mathbb{Z}_m$ (resp. $\bar{\beta} \in \mathbb{Z}_n$), les classes inversibles de \mathbb{Z}_{mn} sont les classes $\overline{vb\alpha + ua\beta}^{mn}$ avec α (resp. β) premier avec m (resp. n).

Exemple 4.19 Si $m = 7$ et $n = 11$, $u = -3, v = 2$ conviennent, et les classes inversibles de \mathbb{Z}_{77} sont donc celles des : $22\alpha - 21\beta$ pour $\alpha = \pm 1, \pm 2, \pm 3$ et $\beta = \pm 1, \pm 2, \pm 3, \pm 4, \pm 5$. Nous ne ferons pas la liste des $6.10 = 60$ classes ainsi obtenues.

Corollaire 4.20 Si $n > 0$ est entier, et a pour décomposition en facteurs premiers : $n = p_1^{r_1} \dots p_s^{r_s}$, alors $\varphi(n) = (1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_s}) \cdot n$

Théorème 4.21 Soit $n > 0$ entier. Alors : $\sum_{d|n} \varphi(d) = n$. (La somme est prise sur tous les diviseurs de n , 1 et n inclus).

Démonstration : Soit E l'ensemble des couples (d, k) constitués d'un diviseur d de n et d'un entier k premier avec d et compris entre 1 et d . Le cardinal de E est donc $\sum_{d|n} \varphi(d)$. On note $[1, n]$ l'ensemble des entiers compris entre 1 et n . Son cardinal est donc n . Soit $f : E \rightarrow [1, n]$ l'application définie par $f(d, k) := k \cdot (\frac{n}{d})$. On va montrer que f est bijective, ce qui établira le résultat. Observons que si $m = k \cdot (\frac{n}{d})$, et si on note $d' := \frac{n}{d}$, alors $(n, m) = (dd', kd') = d' \cdot (d, k) = d'$, donc $d = \frac{n}{(n, m)}$ et $k = \frac{m}{(n, m)}$. Donc f est injective. De plus, si $m \in [1, n]$ est arbitraire et si on définit : $(d, k) := (\frac{n}{(n, m)}, \frac{m}{(n, m)})$, alors $(d, k) \in E$, et $f(d, k) = \frac{n}{(n, m)} \cdot \frac{m}{(n, m)} = (n, m) \cdot \frac{m}{(n, m)} = m$.
□

4.6 Exercices.

Exercice 4.22 Soit n, m des entiers strictement positifs, avec n diviseur de m . On note N (resp. M) l'ensemble des diviseurs premiers de n (resp. des diviseurs premiers de m qui ne divisent pas n). Donc M peut être vide. On rappelle que $\varphi(n) = n \cdot \prod_{p \in N} (1 - \frac{1}{p})$.

1. Montrer que l'on peut écrire de façon unique $m = n \cdot n' \cdot m'$, de telle sorte que les nombres premiers qui divisent n' (resp. m') soient contenus dans N (resp. M).
2. En déduire que $\varphi(n \cdot n') = n' \cdot \varphi(n)$ et que $\varphi(m) = n' \cdot \varphi(n) \cdot \varphi(m')$.
3. Montrer que $\varphi(n)$ divise $\varphi(m)$.
4. En déduire que $\varphi(m) = \varphi(n)$ si et seulement si : soit $m = n$, soit $m = 2n$ avec n impair.

Exercice 4.23 Soit $n > 1$ entier. Alors la somme des fractions positives irréductibles $\frac{a}{n}$, avec : $0 < a < n$ est égale à $\frac{\varphi(n)}{2}$.

Exercice 4.24 A. Soit a, b, c des entiers positifs tels que $\text{pgcd}(a, b, c) \neq 1$. Alors aucune des fractions $\frac{a+jb}{c}$, avec $j \geq 0$ n'est irréductible.

B*. Soit a, b, c des entiers positifs tels que $\text{pgcd}(a, b, c) = 1$. Il y a alors $\frac{\varphi(bc)}{\varphi(b)}$ fractions irréductibles parmi les $\frac{a+jb}{c}$, avec $j = 0, \dots, c-1$.

Exercice 4.25 On rappelle que, si $N > 0$ est entier, $\varphi(N)$ désigne le nombre d'entiers premiers à $N > 0$ dans tout intervalle de la forme $[a, a + N[$.

Combien de nombres entiers premiers avec $N = 700$ y-a-t-il dans chacun des intervalles A, B, C suivants ?

- A. $[77, 777]$
- B. $[152, 1552]$
- C. $[154, 1552]$.

Exercice 4.26 On rappelle que, pour tout entier $N > 1$, $\frac{\varphi(N)}{N} = \prod_p (1 - \frac{1}{p})$, où p décrit l'ensemble des nombres premiers qui divisent N .

Soit $m > 1$ et $n > 1$ des entiers, et $d := (m, n)$ leur PGCD.

1. Montrer que $\frac{\varphi(m.n)}{\varphi(m).\varphi(n)} = \frac{d}{\varphi(d)}$ (Décomposer en facteurs premiers).
2. Montrer que m et n sont premiers entre eux si $\varphi(m.n) = \varphi(m).\varphi(n)$.

Exercice 4.27 1. Montrer que $(p - 1)^2 > p$ si $p \geq 3$ est entier.

En déduire que :

2. $(1 - \frac{1}{p}) \geq \frac{1}{\sqrt{p}}$ pour tout $p \geq 3$.
3. $\frac{\varphi(n)}{n} \geq \frac{1}{\sqrt{2n}}$ pour tout entier $n > 0$.
4. Pour tout entier $m > 0$, l'équation $\varphi(n) = m$, d'inconnue n , a, au plus, $2m^2$ solutions.

Exercice 4.28 1. Montrer que $\varphi(n)$ est pair si $n > 2$.

2. Montrer que pour tout entier pair $0 < m$, l'équation $\varphi(n) = 2m$ d'inconnue n a un nombre fini (que l'on majorera) de solutions.

3. Déterminer les entiers $n > 2$ pour lesquels $\varphi(n) \leq 12$.

Exercice 4.29 Montrer les égalités suivantes :

1. $\sum_{d|n} \varphi(d) = n$. (considérer, pour $0 \leq k \leq n$, le pgcd de n et de k).
2. $\sum_{k \leq n} \varphi(k) \binom{n}{k} = \frac{(n+1)n}{2}$. (considérer, pour $0 \leq k \leq n$, l'égalité précédente).

Exercice 4.30 Si $m | n$, montrer que $\varphi(m) | \varphi(n)$.

Exercice 4.31 Si n n'est pas un carré d'entier, et si $(n - 1) > \varphi(n) > n - \sqrt[3]{n^2}$, montrer que n est le produit de deux nombres premiers distincts.

Exercice 4.32 Montrer que, pour tout $n \geq 2$ et tout $r \geq 2$, r divise $\varphi(n^r - 1)$. Le vérifier pour $(n, r) = (3, 3), (7, 3), (2, 11)$.

Exercice 4.33 Montrer que si $(a, m) = 1$, il existe $N \in \mathbb{N}^*$ tel que $a^N \equiv 1[m]$. Trouver N pour $a = 257$ et $m = 72$.

Exercice 4.34 Calculer $\varphi(n)$ et $\lambda(n)$ si $n = 24, 30$, et aussi si $n := 65520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$.

Exercice 4.35 Montrer que les couples $(\varphi(n), \lambda(n))$ sont les mêmes pour les entiers n suivants : $n = 15, 16, 20$ et 30 .

Montrer cette propriété pour $n = 35, 36, 45$.

Montrer que \mathbb{Z}_{16}^* et \mathbb{Z}_{24}^* n'ont pas le même $\lambda(n)$ bien qu'ayant le même cardinal.

Exercice 4.36 Montrer que les ensembles \mathbb{Z}_n^* ont le même cardinal et le même $\lambda(n)$ pour $n = 15, 16, 20$ et 30 .

Montrer les mêmes propriétés pour $n = 35, 36$ et 45 .

Montrer que \mathbb{Z}_{16}^* et \mathbb{Z}_{24}^* ont le même cardinal mais des λ différents.

Exercice 4.37 Si p et $q = 2p + 1$ sont premiers, et si $a, b, c \in \mathbb{Z}$ sont tels que $a^p + b^p = c^p$, montrer que q divise l'un au moins des trois nombres a, b, c .

Si $u, v \in \mathbb{Z}$, on pose : $a := u^2 - v^2$, $b := 2uv$, $c = u^2 + v^2$. Montrer de 2 manières que l'un au moins des nombres a, b, c est divisible par 5. Le ou lesquels (en fonction de u, v) ?

Exercice 4.38 Pour tout entier $m > 2$, montrer que $\varphi(m) \geq 2\sqrt{m}$. Indication : si $p \geq 3$, vérifier que $(p-1) \geq \sqrt{p}$.

Montrer de même que, pour tout $\alpha < 1$, il existe une constante $C(\alpha) > 0$ telle que $\varphi(m) \geq C(\alpha).m^\alpha$. Déterminer une constante $C(\alpha)$ pour $\alpha = 2/3$, et pour $\alpha = 3/4$. Indication : remarquer que la fonction $\psi_\alpha(m) := \frac{\varphi(m)}{m^\alpha}$ est multiplicative.

Exercice 4.39 * Les p_j étant des nombres premiers distincts ordonnés de façon croissante, on pose : $P = p_1 \dots p_r$. Montrer que :

1. $\prod_j (1 + \frac{1}{p_j}) \leq \sum_{m=1}^{m=P} \frac{1}{m} \leq (1 + \text{Log}(P))$. Indication : pour la première inégalité : développer le produit, pour la seconde, comparer à l'intégrale de $f(x) := \frac{1}{x}$ prise entre 1 et P .

2. $\prod_j \frac{1}{(1 - \frac{1}{p_j^2})} \leq \sum_{m=1}^{m=+\infty} \frac{1}{m^2} \leq (1 + \sum_{m=2}^{m=+\infty} \frac{1}{m(m-1)}) = 2$.

3. $\prod_j \frac{1}{(1 - \frac{1}{p_j})} \leq 2.(1 + \text{Log}(P))$. (Ecrire : $\frac{1}{(1 - \frac{1}{p_j})} = \frac{(1 + \frac{1}{p_j})}{(1 - \frac{1}{p_j^2})}$)

4. $\varphi(n) \geq \frac{n}{2.(1 + \text{Log}n)}$ pour tout $n > 1$. Comparer ce résultat avec celui de l'exercice précédent.

Exercice 4.40 Pour tout entier $m > 2$, montrer que $\varphi(m) \geq 2\sqrt{m}$. Indication : si $p \geq 3$, vérifier que $(p-1) \geq \sqrt{p}$.

Montrer de même que, pour tout $\alpha < 1$, il existe une constante $C(\alpha) > 0$ telle que $\varphi(m) \geq C(\alpha).m^\alpha$. Déterminer une constante $C(\alpha)$ pour $\alpha = 2/3$, et pour $\alpha = 3/4$. Indication : remarquer que la fonction $\psi_\alpha(m) := \frac{\varphi(m)}{m^\alpha}$ est multiplicative.

Exercice 4.41 * Les p_j étant des nombres premiers distincts ordonnés de façon croissante, on pose : $P = p_1 \dots p_r$. Montrer que :

1. $\prod_j (1 + \frac{1}{p_j}) \leq \sum_{m=1}^{m=P} \frac{1}{m} \leq (1 + \text{Log}(P))$. Indication : pour la première inégalité : développer le produit, pour la seconde, comparer à l'intégrale de $f(x) := \frac{1}{x}$ prise entre 1 et P .

2. $\prod_j \frac{1}{(1 - \frac{1}{p_j^2})} \leq \sum_{m=1}^{m=+\infty} \frac{1}{m^2} \leq (1 + \sum_{m=2}^{m=+\infty} \frac{1}{m(m-1)}) = 2$.

3. $\prod_j \frac{1}{(1 - \frac{1}{p_j})} \leq 2.(1 + \text{Log}(P))$. (Ecrire : $\frac{1}{(1 - \frac{1}{p_j})} = \frac{(1 + \frac{1}{p_j})}{(1 - \frac{1}{p_j^2})}$)

4. $\varphi(n) \geq \frac{n}{2.(1 + \text{Log}n)}$ pour tout $n > 1$. Comparer ce résultat avec celui de l'exercice précédent.

4.7 *Fonctions multiplicatives.

Definition 4.42 Une fonction $f : \mathbb{N} \rightarrow \mathbb{C}$ est dite **multiplicative** si $f(m.n) = f(m).f(n)$ lorsque $(m, n) = 1$.

Exemple 4.43 1. La fonction φ est multiplicative, par le théorème ??.

2. La fonction de Möbius $\mu : \mathbb{N} \rightarrow \mathbb{Z}$ définie par : $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier, et par $\mu(n) = (-1)^s$ si n est le produit de $s \geq 0$ facteurs premiers distincts, est multiplicative.

Remarque 4.44 Si f est multiplicative (non nulle), on a donc : $f(1) = 1$ et $f(n) = f(p_1^{r_1}) \dots f(p_s^{r_s})$ si la décomposition de n en facteurs premiers est : $n = p_1^{r_1} \dots p_s^{r_s}$. Une fonction multiplicative est donc déterminée par ses valeurs sur les p^r , qui peuvent être choisis arbitrairement.

Exemple 4.45 Les fonctions suivantes sont multiplicatives :

1. Si f est multiplicative, alors $g(n) := \sum_{\{d|n\}} f(d)$ est multiplicative, puisque si $(m, n) = 1$, tout diviseur D de $m.n$ s'écrit de manière unique comme $D = d'.d$, avec d (resp. d') diviseur de m (resp. n). La somme porte sur tous les diviseurs d de n , 1 et n compris. On en déduit que :

2. Les fonctions $\tau(n) := \sum_{\{d|n\}} 1$ comptant le nombre de diviseurs de n , et $\sigma_k := \sum_{\{d|n\}} d^k$, $k \geq 0$ entier, égal à la somme des puissances k -ièmes des diviseurs de n , sont multiplicatives. (On a donc : $\sigma_0 = \tau$).

De plus : $\sigma_k(p^r) = (1 + p^k + p^{2k} + \dots + p^{r.k}) = \frac{p^{r.k+1} - 1}{p^k - 1}$ si $k > 0$, et $\tau(p^r) = (r + 1)$ si $k = 0$. Donc : $\tau(n) = (r_1 + 1) \dots (r_s + 1)$ si n est décomposé comme ci-dessus en facteurs premiers.

3. La fonction $\sum_{\{d|n\}} \mu(d)$ est donc multiplicative. Elle vaut 1 si $n = 1$, et vaut $0 = 1 - 1$ lorsque $n = p^r$ est une puissance de nombre premier. Elle vaut donc 0 pour tout $n > 1$.

4. On en déduit la **formule d'inversion de Moebius** : si $f(n)$, $n \geq 1$ est une fonction (multiplicative ou non), et $g(n) := \sum_{\{d|n\}} f(d)$, alors : $f(n) = \sum_{\{d|n\}} \mu(d).g(\frac{n}{d}) = \sum_{\{d|n\}} \mu(\frac{n}{d}).g(d)$.

En effet : $\sum_{\{d|n\}} \mu(\frac{n}{d}).g(d) = \sum_{\{d'|d|n\}} \mu(\frac{n}{d}).f(d') = \sum_{\{d'|n\}} f(d').(\sum_{\{\frac{n}{d}|\frac{n}{d'}\}} \mu(\frac{n}{d}))$. Or, $\sum_{\{\frac{n}{d}|\frac{n}{d'}\}} \mu(\frac{n}{d}) = 0$ sauf si $(\frac{n}{d} = 1)$, ce qui implique le résultat.

Corollaire 4.46 Pour tout $n > 1$ on a : $\sum_{\{d|n\}} \mu(d).(\frac{n}{d}) = \varphi(n)$.

Démonstration : Appliquer la formule d'inversion de Moebius au théorème ??
□

4.8 Exercices.

Exercice 4.47 Montrer de deux façons, si $n \geq 1$ est entier, que : $\sum_{\{d|n\}} \mu(d).(\frac{n}{d}) = \varphi(n)$. Indication : ou bien utiliser l'inversion de Möbius, ou bien observer que cette somme est une fonction multiplicative.

Montrer de même, si $N, n \geq 1$ sont entiers, que : $\sum_{\{d|n; (d, N)=1\}} \mu(d).(\frac{n}{d}) = \frac{\varphi(n.N)}{\varphi(N)}$.

Exercice 4.48 *

Montrer de même, si $N, n \geq 1$ sont entiers, que : $\sum_{\{d|n; (d, N)=1\}} \mu(d) \cdot \left(\frac{n}{d}\right) = \frac{\varphi(n \cdot N)}{\varphi(N)}$.

Exercice 4.49 Soit $h : \mathbb{N} \rightarrow \mathbb{C}$ une fonction. On définit, pour $n > 0$ entier : $f(n) := \sum_{\{1 \leq a \leq n | a \in \mathbb{N}\}} h(n)$, et $g(n) := \sum_{\{1 \leq a \leq n | a \in \mathbb{N}, (a, n)=1\}} h(n)$. Montrer que $f(n) = \sum_{\{d|n\}} g\left(\frac{n}{d}\right)$. En déduire que $g(n) = \sum_{\{d|n\}} \mu\left(\frac{n}{d}\right) \cdot f(d)$.

Exercice 4.50 * Soit $c(m, n) := \sum_{\{1 \leq a \leq n | a \in \mathbb{N}, (a, n)=1\}} e^{\frac{2i\pi am}{n}}$, pour m, n entiers positifs. On pose : $h(a) := e^{\frac{2i\pi am}{n}}$ si $a \in \mathbb{N}$. Calculer les fonctions f et g associées dans l'exercice 4.49, et en déduire que $c(m, n) = \sum_{d|\delta} \mu\left(\frac{n}{d}\right) \cdot d$, si $\delta := (m, n)$.

Montrer ensuite que $c(m, n) = \delta \cdot \mu\left(\frac{n}{\delta}\right) \cdot \frac{\varphi(n)}{\varphi(n')}$, si $n = n' \cdot \delta$. Indication : écrire $c(m, n) = \sum_{c, d=\delta} \mu\left(n' \cdot \left(\frac{\delta}{c}\right)\right) \cdot d = \sum_{c, d=\delta} \mu\left(n' \cdot c\right) \cdot \left(\frac{\delta}{c}\right)$. Utiliser ensuite le fait que, pour tout entier $k > 0$, ou bien $\mu(n' \cdot k) = 0$, ou bien $\mu(n' \cdot k) = \mu(n') \cdot \mu(k)$. Conclure avec 4.47.

Exercice 4.51 Soit $S(n)$ la somme des entiers $1 \leq a < n$ et premiers à n . Montrer que $S(n) = n \cdot \frac{\varphi(n)}{2}$ si $n > 1$. Indication : considérer a et $(n - a)$.

Exercice 4.52 * 1. Soit $F_k(n) := 1^k + 2^k + \dots + n^k$, pour $n \geq 1$ entier. Calculer $F_1(n)$ et montrer (par récurrence sur n) que $F_3(n) = (F_1(n))^2$ pour tout $n \geq 1$.

Pour $n > 1$, soit $f_k(n) := \sum_{\{1 \leq a \leq n | (a, n)=1\}} \frac{a^k}{n^k}$, et $g_k(n) := \sum_{\{d|n\}} f_k(d)$.

2. Montrer que $g_k(n) = F_k(n)$ pour tout $n > 1$. Indication : associer à tout entier $1 \leq x \leq n$ le couple (x', n') , avec $x' := \frac{x}{d}$, $n' := \frac{n}{d}$, $d := \text{pgcd}(x, n)$.

3. Retrouver le résultat de l'exercice précédent en utilisant la formule d'inversion de Moebius.

4. Montrer, à l'aide de la formule d'inversion de Moebius et de l'exercice 4.47, que, pour tout $n > 1$, on a : $f_3(n) = \frac{\varphi(n)}{4} \cdot (1 + (-1)^s \cdot \frac{p_1 \dots p_s}{n^2})$ si les nombres premiers divisant n sont p_1, \dots, p_s .

5. Calculer $f_2(n)$ en fonction de $f_3(n)$ en utilisant l'indication de l'exercice précédent.

Exercice 4.53 Si $n > 1$ entier, on note $P(n)$ le produit des entiers a compris entre 1 et n , et premiers avec n . Montrer que $P(n) = n^{\varphi(n)} \cdot \prod_{\{0 < d|n\}} \left(\frac{d!}{d^d}\right)^{\mu(d)}$. Indication : procéder (multiplicativement) comme dans l'exercice 4.52.2.

4.9 Généralisation d'Euler du petit théorème de Fermat.

Théorème 4.54 Pour tout $a \in \mathbb{Z}$ et tout $n > 0$ entier, $a^{\varphi(n)} \equiv 1[n]$ si $(a, n) = 1$. De manière équivalente : $\bar{a}^{\varphi(n)} = \bar{1}$ dans \mathbb{Z}_n si $\bar{a} \in \mathbb{Z}_n^*$.

Démonstration : Soit $\bar{P} \in \mathbb{Z}_n^*$ le produit de tous les éléments $x_1, x_2, \dots, x_{\varphi(n)}$ de \mathbb{Z}_n^* , pris dans un ordre quelconque. Alors les éléments $\bar{a} \cdot x_1, \bar{a} \cdot x_2, \bar{a} \cdot x_3, \bar{a} \cdot x_4, \dots, \bar{a} \cdot x_{\varphi(n)}$ forment une permutation des éléments $x_1, x_2, \dots, x_{\varphi(n)}$, puisqu'ils sont deux-à-deux distincts (puisque $\bar{a} \cdot x = \bar{a} \cdot y$ implique $x = y$ si $x \neq y \in \mathbb{Z}_n^*$). Leur produit est donc égal à \bar{P} , et aussi à $\bar{a}^{\varphi(n)} \cdot \bar{P}$. On en déduit que $\bar{a}^{\varphi(n)} = \bar{1}$, puisque $\bar{P} \in \mathbb{Z}_n^*$. \square

Remarque 4.55 *L'exposant $\varphi(n)$ du théorème d'Euler (mais non celui du théorème de Fermat) peut être, en général considérablement amélioré. Ceci est dû au fait qu'il n'y, en général, pas de racine primitive modulo n . (Voir §?? ci-dessous). La formulation optimale est la suivante :*

Théorème 4.56 *Soit $n = 2^r \cdot p_1^{r_1} \dots p_s^{r_s}$ la décomposition de n en facteurs premiers. Soit $a \geq 1$ entier tel que $(a, n) = 1$. Alors $a^{\lambda(n)} \equiv 1[n]$, avec $\lambda(n) := \text{ppcm}\{2^\sigma, \varphi(p_1^{r_1}), \dots, \varphi(p_s^{r_s})\}$, où $\sigma := r - 1$ si $r \leq 2$, et $\sigma := r - 2$ si $r \geq 3$. Remarquons que $\lambda(n)$ divise évidemment $\varphi(n)$.*

Démonstration : Supposons d'abord que $n = 2^r$. Si $r = 1, 2$, l'assertion résulte du théorème d'Euler. Si $r \geq 3$, remarquons que $(1 + 2x)^2 = 1 + 4x + 4x^2 = 1 + 8y$, pour tout x entier, avec $y = x^2 + x$. Donc $(1 + 2x)^{2^k} = (1 + 8y)^{2^{k-1}} = 1 + 2^{k+2}z$, pour tout entier $k \geq 1$, par récurrence sur k .

En effet, $(1 + 2x)^{2^{k+1}} - 1 = (1 + 2x)^{2^k} - 1 \cdot (1 + 2x)^{2^k} + 1$. Voir aussi l'argument de ?? pour plus de détails.

Il en résulte que, si $r \geq 3$, alors $u^{2^{r-2}} = \bar{1}$, pour tout élément u de $\mathbb{Z}_{2^r}^*$.

Nous traitons maintenant le cas général, où $n = 2^r \cdot p_1^{r_1} \dots p_s^{r_s}$. Par définition de $\lambda(n)$, on a, pour tout $a \in \mathbb{Z}_n^*$, $a^{\lambda(n)} \equiv 1[p_j^{r_j}]$ pour tout $j = 1, 2, \dots, s$, et aussi modulo $[2^r]$, par ce qui précède, donc $a^{\lambda(n)} \equiv 1[n] \square$

Exemple 4.57

1. Par Euler : $a^{64} = 1$ dans \mathbb{Z}_{240}^* , si $(a, 240) = 1$, car $\varphi(240) = \varphi(2^4 \cdot 3 \cdot 5) = 2^3 \cdot 2 \cdot 4 = 64$. Cependant $\lambda(240) = \text{ppcm}\{2^2, 2, 2^2\} = 4$. Donc $a^4 \equiv 1[240]$. En effet : a est alors premier avec 16, 3 et 5. Donc $(a^4 - 1)$ est divisible par 3 et 5, par Fermat, et aussi par 16 (voir ci-dessous). Donc aussi par 240, leur produit (lemme d'Euclide). Vérifions l'assertion pour $n = 16$: si a est impair, $(a^2 - 1) \equiv 0[8]$, puisque $a^2 \equiv 1^2, 3^2[8]$. Donc $a^2 \equiv 1, 9[16]$. Or $9^2 \equiv 1[16]$. Donc $a^4 \equiv 1[16]$.

2. De la même façon, on vérifie que $a^{12} \equiv 1[6552]$ si $(a, 6552) = 1$, alors que $\varphi(6552) = 12^3 = 1728$ puisque $6552 = 2^3 \cdot 3^2 \cdot 7 \cdot 13$.

Remarque 4.58 *L'exposant $\lambda(n)$ ne peut être amélioré (simultanément pour tous les éléments de \mathbb{Z}_n^*). Ceci résulte du fait qu'il existe toujours un élément $\bar{a} \in \mathbb{Z}_n^*$ dont l'ordre multiplicatif est $\lambda(n)$. Voir ?? et ??.*

4.10 *Ordre multiplicatif d'un élément de \mathbb{Z}_n^* .

Soit $n > 1$ entier, $a \in \mathbb{Z}$, premier avec n , et $\bar{a} \in \mathbb{Z}_n^*$ son image dans \mathbb{Z}_n . Si $k \in \mathbb{Z}$, on note \bar{a}^k sa puissance k -ième dans \mathbb{Z}_n^* , définie comme le produit de $|k|$ termes tous égaux à \bar{a} si $k \geq 0$, et égaux à \bar{a}^{-1} sinon. On a donc : $\bar{a}^{k+k'} = \bar{a}^k \cdot \bar{a}^{k'}$, pour tous $k, k' \in \mathbb{Z}$.

De plus : $\bar{a}^{\varphi(n)} = \bar{1}, \forall \bar{a} \in \mathbb{Z}_n^*$, par le théorème d'Euler, et même, plus précisément : $\bar{a}^{\lambda(n)} = \bar{1}, \forall \bar{a} \in \mathbb{Z}_n^*$, d'après 4.56.

Definition 4.59 Soit $\bar{a} \in \mathbb{Z}_n^*$ un élément inversible de \mathbb{Z}_n , si $n > 1$ est entier. L'ordre de $\bar{a} \in \mathbb{Z}_n^*$, noté $o_n(\bar{a})$ est le plus petit des entiers $m > 0$ tel que $\bar{a}^m = \bar{1} \in \mathbb{Z}_n$. Si $a \in \mathbb{Z}$ est tel que $(a, n) = 1$, on note aussi $o_n(a)$ l'ordre de $\bar{a}^{(n)} \in \mathbb{Z}_n$.

Exemple 4.60 $o_n(\bar{a}) = 1$ si et seulement si $\bar{a} = \bar{1}$, ceci pour tout $n > 1$.

Proposition 4.61 Soit $\bar{a}, \bar{b} \in \mathbb{Z}_n^*$.

1. Si $m > 0$ est entier, alors $\bar{a}^m = \bar{1} \in \mathbb{Z}_n$ si et seulement si $o_n(\bar{a})$ divise m .
2. $\bar{a}^k = \bar{a}^\ell$ si et seulement si $k \equiv \ell$ modulo $o_n(\bar{a})$.
3. $o_n(\bar{a})$ divise $\lambda(n)$ (qui divise $\varphi(n)$), pour tout $\bar{a} \in \mathbb{Z}_n^*$.
4. Pour tout entier $k > 0$, $o_n(\bar{a}^k) = \frac{o_n(\bar{a})}{(k, o_n(\bar{a}))}$.
5. Si $o_n(\bar{a})$ et $o_n(\bar{b})$ sont premiers entre eux, alors $o_n(\bar{a}.\bar{b}) = o_n(\bar{a}).o_n(\bar{b})$.
6. Si $n = m.m'$ avec $(m, m') = 1$, alors $o_n(\bar{a}) = o_m(\bar{a}) \cap o_{m'}(\bar{a})$, pour tout $a \in \mathbb{Z}$.

Démonstration : Soit $m := o_\times(\bar{a})$. Soit $k = qm + r$ la division euclidienne de $(k - \ell)$ par m . On a donc : $\bar{1} = \bar{a}^{(k-\ell)} = (\bar{a}^m)^q . \bar{a}^r = \bar{1}^q . \bar{a}^r = \bar{a}^r$. Puisque $0 \leq r < m$, la minimalité de m parmi les exposants $s > 0$ tels que $\bar{a}^s = \bar{1}$ implique que $r = 0$ et donc que m divise $(k - \ell)$. D'où l'assertion 0, dont l'assertion 1 est le cas particulier où $\ell = 0$.

Par le théorème d'Euler, $\bar{a}^{\varphi(n)} = \bar{1}$, donc m divise $\varphi(n)$. D'où 2.

Pour l'assertion 3 : si $b := \bar{a}^k$, et si $m := o_\times(\bar{a})$, alors $b^{\frac{m}{k}} = \bar{a}^m = \bar{1}$. Donc $\ell := o_\times(b)$ divise $\frac{m}{k}$. Réciproquement, si $\bar{1} = b^\ell = a^{k.\ell}$, on a : m divise $k.\ell$, donc $\frac{m}{k}$ divise ℓ . D'où 3.

La dernière assertion résulte de ce que $a^k \equiv 1[N]$ si et seulement si $a^k \equiv 1[m]$ et $a^k \equiv 1[n]$, donc si et seulement si k est divisible par $o_{\times, m}(\bar{a})$ et $o_{\times, n}(\bar{a})$, donc par leur ppcm \square

Corollaire 4.62 Si $n = p_1^{r_1} \dots p_s^{r_s}$ est la décomposition de n en facteurs premiers, et si $(a, n) = 1$, alors l'ordre de a modulo n est le ppcm des ordres de a modulo $p_j^{r_j}$, pour $j = 1, \dots, s$.

4.11 Exercices.

Exercice 4.63 Calculer $o_\times(\bar{a})$ pour $\bar{a} \in \mathbb{Z}_n^*$, si $n = 3, 4, 5, 6, 7, 8, 9, 11, 13$.

Exercice 4.64 Calculer $o_\times(17)$ modulo 1001.

Exercice 4.65 Déterminer $d := \text{pgcd}(A, B)$, avec : $A := m^a - 1, B := m^b + 1$ si $m, a, b > 1$ sont entiers, et a impair. Indication : déterminer le reste de la division par d de $m^{ab} = (A + 1)^b = (B - 1)^a$. Seconde méthode : si p est un diviseur premier de d , considérer l'ordre multiplicatif de m modulo p

Exercice 4.66 Si a est premier avec $n > 2$, et si b, c sont des entiers positifs, montrer que si $a^b \equiv -1[n]$, et si $a^c \equiv \pm 1[n]$, alors $a^d \equiv -1[n]$, et que $\frac{b}{d}$ est impair, avec $d := (b, c)$.

Exercice 4.67 Montrer que si $p \equiv 1 \pmod{8}$, le groupe \mathbb{Z}_8^* a un élément u d'ordre 8. Montrer que $u^4 = -1$, puis que $v := u + u^{-1}$ vérifie $v^2 = 2$. En déduire que 2 est un carré modulo p .

Exercice 4.68 Montrer que $p \equiv 1 \pmod{8}$, si p , premier, divise un nombre n de la forme : $n = a^4 + 1$. Montrer l'existence d'une infinité de nombres premiers p non congrus à 1 modulo 8, mais divisant des nombres de la forme : $m = a^8 - 1$.

Exercice 4.69 Montrer que, pour tout $n \geq 2$ et tout $r \geq 2$, r divise $\varphi(n^r - 1)$. Le vérifier pour $(n, r) = (3, 3), (7, 3), (2, 11)$.

Exercice 4.70

1. Montrer que si $k - 1$ est divisible par $p - 1$, p premier, alors $ab(a^k - b^k) \equiv 0 \pmod{p}$ quels que soient $a, b \in \mathbb{Z}$.
2. Déduire de 1. que $2.3.5.7.11.13.31.61 = 56786730$ divise $ab(a^{60} - b^{60})$.
3. Formuler des résultats analogues si l'exposant 60 est remplacé par 6, 12, 24 ou 30.

Exercice 4.71 Montrer que, pour tout $n \in \mathbb{Z}$, $3^{n+3} \equiv 4^{4n+2} \pmod{11}$.

Exercice 4.72 Déterminer le reste de la division de 37^n par 11 pour $n \in \mathbb{N}$. Combien de cas faut-il considérer ?

Exercice 4.73 Montrer que si $(a, m) = 1$, il existe $N \in \mathbb{N}^*$ tel que $a^N \equiv 1 \pmod{m}$. Trouver N pour $a = 257$ et $m = 72$.

Exercice 4.74 Montrer que $n^5 - n$ est toujours divisible par 30 si $n \in \mathbb{Z}$.

Exercice 4.75 Montrer que l'équation $x^2 = 1$ a dans \mathbb{Z}_n :

1. seulement les deux solutions $x = \pm 1$ si $n = p^r$, p premier impair, ou si $n = 2.p^r$.
2. exactement 2^s solutions si n est impair divisible par r nombres premiers distincts.

Exercice 4.76 Déterminer les nombres de trois chiffres congrus à 4 modulo 7, 9 et 11.

Exercice 4.77 Trouver le reste de la division de 6647^{362} par $n = 7785562197230017200 = 2^4.3^2.5^2.7.11.13.19.31.37.41.61.73.181$.

Exercice 4.78 Montrer que si $(a, m) = 1$, il existe $N \in \mathbb{N}^*$ tel que $a^N \equiv 1 \pmod{m}$. Trouver N pour $a = 257$ et $m = 72$.

Exercice 4.79 Calculer $\varphi(n)$ et $\lambda(n)$ si $n = 24, 30$, et aussi si $n := 65520 = 2^4.3^2.5.7.13$.

Exercice 4.80 Montrer que les couples $(\varphi(n), \lambda(n))$ sont les mêmes pour les entiers n suivants : $n = 15, 16, 20$ et 30 .

Montrer cette propriété pour $n = 35, 36, 45$.

Montrer que \mathbb{Z}_{16}^* et \mathbb{Z}_{24}^* n'ont pas le même $\lambda(n)$ bien qu'ayant le même cardinal.

Exercice 4.81 Montrer que les ensembles \mathbb{Z}_n^* ont le même cardinal et le même $\lambda(n)$ pour $n = 15, 16, 20$ et 30 .

Montrer les mêmes propriétés pour $n = 35, 36$ et 45 .

Montrer que \mathbb{Z}_{16}^* et \mathbb{Z}_{24}^* ont le même cardinal mais des λ différents.

Exercice 4.82 Si p et $q = 2p + 1$ sont premiers, et si $a, b, c \in \mathbb{Z}$ sont tels que $a^p + b^p = c^p$, montrer que q divise l'un au moins des trois nombres a, b, c .

Si $u, v \in \mathbb{Z}$, on pose : $a := u^2 - v^2$, $b := 2uv$, $c = u^2 + v^2$. Montrer de 2 manières que l'un au moins des nombres a, b, c est divisible par 5. Le ou lesquels (en fonction de u, v) ?

5 Sujet du partiel d'octobre 2009.

Université Nancy 1. Examen arithmétique et algèbre du 23/10/09.

Durée : 2h. Documents et calculatrice interdits.

Exercice 5.1 L'équation $3x + 18y = 2$ a-t-elle des solutions $(x, y) \in \mathbb{Z}^2$? (Si "oui" : les déterminer, si "non" : dire pourquoi).

Exercice 5.2 Déterminer le PGCD de $m = 1729$ et de $n = 2431$, puis décomposer ces deux nombres en produits de facteurs premiers.

Exercice 5.3 Montrer que $\overline{17}$ est inversible dans \mathbb{Z}_{71} , et déterminer son inverse.

Exercice 5.4 Déterminer les entiers $n \in \mathbb{Z}$ satisfaisant les systèmes de congruences A , puis B suivants :

A. $n \equiv 3[11]$ et $n \equiv 2[17]$. (On pourra écrire : $n = 3 + 11k, k \in \mathbb{Z}$).

B. $n \equiv 3[11]$, $n \equiv 2[17]$, et $n \equiv 4[7]$.

Exercice 5.5 Déterminer (presque sans calcul) le reste des divisions euclidiennes de N par d si :

1. $N = 1000^n$ par $d = 1001$, pour tout $n \geq 0$ entier.

2. $N = 259137820527$ par $d = 1001$. (On pourra écrire N sous la forme : $N = 527 + 820 \cdot (1000) + 137 \cdot (1000)^2 + 259 \cdot (1000)^3$).

3. $N = 259137820527$ par $d = 7, 11$, et 13 . (Noter que $1001 = 7 \cdot 11 \cdot 13$).

Exercice 5.6

A. Soit $q > 2$ un nombre premier impair. Montrer que :

1. pour tous $a, b \in \mathbb{Z}$, $(a + b)^q \equiv a^q + b^q[q]$. (Rappel : $C_q^j \equiv 0[q]$ pour $0 < j < q$).

2. $2^q \equiv 2[q]$ et $2^{q-1} \equiv 1[q]$.

Soit, de plus, $n > 0$ un entier tel que $2^n \equiv 1[q]$. Montrer que :

3. pour tous $u, v \in \mathbb{Z}$ entiers, $\bar{2}^m = 1 \in \mathbb{Z}_q$, si $m = u \cdot n + v \cdot (q - 1)$. (On écrira : $2^{u \cdot n} = (2^n)^u$ et $2^{v \cdot (q-1)} = (2^{q-1})^v$).

4. $2^d \equiv 1[q]$ si d est le PGCD de n et de $(q - 1)$.

B. On se donne un entier $n > 1$, et on note q un diviseur premier de $N := 2^n - 1$.

5. Montrer que q est impair, et que $2^n \equiv 1[q]$.

6. Si d est le PGCD de n et de $(q - 1)$, montrer que $2^d \equiv 1[q]$.

7. En déduire que $d > 1$.

Soit p (resp. q_0) le plus petit diviseur premier de n (resp. de $N = 2^n - 1$).

8. Montrer que $p < q_0$. (Choisir $q = q_0$ et noter que p divise d).

9. Si n est pair, montrer que $p = 2$ et que $q_0 = 3$.

10. Déterminer p et q_0 lorsque $n = 3, 5, 7, 9$.

12. Montrer que si $p = 3$, alors $q_0 = 7$.

Exercice 5.7 On rappelle que, si $N > 0$ est entier, $\varphi(N)$ désigne le nombre d'entiers premiers à $N > 0$ dans tout intervalle de la forme $[a, a + N[$.

Combien de nombres entiers premiers avec $N = 700$ y-a-t-il dans chacun des intervalles A, B, C suivants ?

- A. $[77, 777]$
- B. $[152, 1552]$
- C. $[154, 1552]$

Exercice 5.8 On rappelle que, pour tout entier $N > 1$, $\frac{\varphi(N)}{N} = \prod_p (1 - \frac{1}{p})$, où p décrit l'ensemble des nombres premiers qui divisent N .

Soit $m > 1$ et $n > 1$ des entiers, et $d := (m, n)$ leur PGCD.

1. Montrer que $\frac{\varphi(m.n)}{\varphi(m).\varphi(n)} = \frac{d}{\varphi(d)}$ (Décomposer en facteurs premiers).
2. Montrer que m et n sont premiers entre eux si $\varphi(m.n) = \varphi(m).\varphi(n)$.

Barème approximatif : 1+2+2+3+4+10+3+4=29

Université Nancy 1. Examen arithmétique et algèbre du 20/10/10.

Durée : 2h. Documents et calculatrice interdits.

Exercice 5.9 Pour quelles valeurs de $d \in \mathbb{Z}$ l'équation $51x + 19y = d$ a-t-elle des solutions $(x, y) \in \mathbb{Z}^2$? Les déterminer toutes, lorsque $d = 1$.

Exercice 5.10

Exercice 5.11 Montrer que $\overline{13}$ est inversible dans \mathbb{Z}_{31} , et déterminer son inverse.

Exercice 5.12 Déterminer les entiers $n \in \mathbb{Z}$ satisfaisant les systèmes de congruences A , puis B suivants :

A. $2n \equiv 3[11]$ et $3n \equiv 2[17]$.

B. $2n \equiv 3[11]$, $3n \equiv 2[17]$, et $5n \equiv 4[13]$.

Exercice 5.13 Déterminer (presque sans calcul) le reste de la division euclidienne de N par 99 si : $N = (359141)^{359141}$.

Exercice 5.14 Soit $F_n := 2^{2^n} + 1, n \geq 0$ entier le n -ième nombre de Fermat. On pose : $A := 3^{\frac{F_n-1}{2}}$, et on se propose de montrer que F_n est premier si et seulement si $A \equiv -1[F_n]$.

1. Montrer soigneusement que si F_n est premier, alors $A^2 \equiv 1[F_n]$. En déduire que $A \equiv \pm 1[F_n]$, et enfin que $A \equiv -1[F_n]$.

2. Si $A \equiv -1[F_n]$, et si q est un diviseur premier de $A^2 - 1$, montrer que $3^{F_n-1} \equiv 3^{q-1} \equiv 1[q]$. En déduire que $3^d \equiv 1[q]$, si d est le PGCD de $(q-1)$ et de (F_n-1) . En déduire que $q = 2^s$, pour un entier $0 \leq s \leq 2^{n-1}$, puis que $q = F_n$.

3. Peut-on remplacer 3 par d'autres nombres entiers $m > 0$ dans la définition de A ci-dessus, de telle sorte que F_n soit premier si et seulement si $m^{\frac{F_n-1}{2}} \equiv -1[F_n]$? Si oui, par lesquels, et pourquoi ?

Exercice 5.15 Soient m', n' des entiers strictement positifs premiers entre eux.

1. Si $d > 0$ est entier, montrer qu'il existe des entiers strictement positifs μ, ν, δ uniques tels que : $d = \mu \cdot \nu \cdot \delta$, et : $1 = (\mu, n') = (\nu, m') = (\mu, \nu) = (\mu \cdot \nu, \delta) = (m' \cdot n', \delta)$

2. Si m et n sont des entiers strictement positifs, montrer l'existence d'entiers a et b tels que : $a|m, b|n, (\frac{m}{a}, \frac{n}{b}) = 1$, et : $\frac{m}{a} \cdot \frac{n}{b} = m \cap n$. (Observer que $a \cdot b = (m, n) := d$, et que $(\frac{m}{d}, \frac{n}{d}) = 1$).

Exercice 5.16 Soit $a \in \mathbb{Z}$, et $p \neq 3$ un diviseur premier de $N := a^2 + a + 1$.

1. Montrer que $p \equiv 1[6]$.

2. Soit $b := 2a + 1$. Montrer que $b^2 \equiv -3[p]$.

3. Montrer que les conclusions (préciser) subsistent si N et b sont remplacés respectivement par $N' := a^2 - a + 1$ et $b' := 2a - 1$.

4. Trouver $c \in \mathbb{Z}$ tel que $c^2 \equiv -3[p]$ si $p = 37, 13, 19, 73$ (considérer $a = 10, 8$).

5. Trouver $d \in \mathbb{Z}$ tel que $d^2 \equiv 3[p]$ si $p = 37, 13, 73$. (Écrire p comme somme de deux carrés d'entiers).

6. Existe-t-il $d \in \mathbb{Z}$ tel que $d^2 \equiv 3[19]$? Justifier.

Barème approximatif : 1+2+2+3+4+10+3+4=29