**Université Claude Bernard Lyon 1** **Master MAIM (1ère année)**
**Arithmétique et combinatoire** **Année 2011-12**

---

# Feuille 1 :
# Arithmétique élémentaire et congruences

---

**Exercice 1** *Calculer l'inverse de* 13 *modulo* 100.

**Exercice 2** *Résoudre les équations*

$$19x \equiv 2 \pmod{140} \qquad \textit{et} \qquad 57x \equiv 87 \pmod{105}.$$

**Exercice 3** *Résoudre* $42x + 150y = 18$.

**Exercice 4**
1. *Résoudre* $6u + 5z = 10$.
2. *Résoudre* $4x + 5y = u$.
3. *En déduire les solutions de* $24x + 30y + 5z = 10$.

**Exercice 5** Soit $p$ un nombre premier. Montrer que

$$x^2 \equiv 1 \,(\mathrm{mod}\, p)$$

si et seulement si

$$x \equiv \pm 1 \,(\mathrm{mod}\, p).$$

**Exercice 6 (Théorème de Wilson)** Soit $p$ un nombre premier. Le but de l'exercice est de montrer que

$$(p-1)! \equiv -1 \,(\mathrm{mod}\, p).$$

Indication : vérifier d'abord le résultat pour $p = 2, 3$. On suppose alors que $p \geq 5$. Montrer que pour tout $a \in \{1, 2, \ldots, p-1\}$, il existe $a^\sharp \in \{1, 2, \ldots, p-1\}$ tel que $aa^\sharp \equiv 1 \,(\mathrm{mod}\, p)$. Remarquer alors que $a = a^\sharp$ si et seulement si $a = 1$ ou $a = p-1$ (voir exercice 5). Partitionner alors l'ensemble $\{2, \ldots, p-2\}$ en $(p-3)/2$ pairs d'entiers $(a_i, a_i^\sharp)$ tels que $a_i a_i^\sharp \equiv 1 \,(\mathrm{mod}\, p)$ pour $1 \leq i \leq (p-3)/2$. Conclure.

**Exercice 7** *Le produit de trois entiers consécutifs peut–il être un carré ?*

**Exercice 8**
1. *Montrer que, pour tout* $n \in \mathbb{N}$, $n^{13} - n$ *est multiple de* 455.
2. *Montrer qu'on peut améliorer ce résultat, c'est-à-dire qu'il existe un multiple non trivial de* 455 *qui divise tous les* $n^{13} - n$.
3. *Quel est le plus grand entier* $m$ *qui divise tous les* $n^{13} - n$ *?*

**Exercice 9** *On définit la suite des nombres de Fermat par* $F_n = 2^{2^n} + 1$.
1. *Montrer que les* $F_n$ *sont deux à deux premiers entre eux.*
   *Indication : si* $m < n$ *alors* $F_m$ *divise* $F_n - 2$.
2. *En déduire qu'il existe une infinité de nombres premiers.*

**Exercice 10** *Prouver qu'il existe une infinité de premiers de la forme* $4k-1$. *Prouver de la même façon qu'il existe une infinité de nombres premiers de la forme* $6k-1$.

**Exercice 11** *Expliciter un $n$ tel que $n, n+1, n+2, \ldots, n+9$ soient tous non premiers.*

**Indication :** *on pourra traduire le problème comme un système de congruences et utiliser le théorème des restes chinois.*

**Exercice 12** *$a$ et $b$ sont premiers entre eux et $N \in \mathbb{N}$. On considère l'équation*

$$ax + by = N \qquad (E)$$

1. *Montrer que si $N$ est assez grand l'équation $(E)$ a une solution en entiers naturels.*
2. *Montrer que si $N = (a-1)(b-1) - 1$ l'équation $(E)$ n'a pas de solutions en entiers naturels.*
3. *Montrer que si $N \geq (a-1)(b-1)$ l'équation $(E)$ a une solution en entiers naturels.*

**Exercice 13** *Soient $x_1, x_2, \ldots, x_n$ des entiers relatifs. Montrer qu'il existe $i, j$ entiers, $1 \leq i < j \leq n$ tels que $x_i + x_{i+1} + \cdots + x_j \equiv 0 \pmod{n}$.*

**Indication :** *on pourra introduire*

$$S_j = \sum_{0<i\leq j} x_j \bmod n$$

*et applique le principe des tiroirs de Dirichlet.*

**Exercice 14** *Vérifier que les 4 derniers chiffres (en base 10) de $9376^2$ sont 9376. Déterminer tous les entiers $x$, $0 \leq x < 10000$ tels que $x^2 \equiv x \pmod{10000}$ ?*

**Indication :** *on pourra remarquer que $x$ est solution de $X^2 - X \equiv 0 \pmod{N}$ si et seulement si $1 - x$ est solution.*

**Exercice 15** *Résoudre le système de congruences*

$$\begin{cases} 2x & \equiv & 3 & \pmod 5 \\ 4x & \equiv & 3 & \pmod 7 \\ 3x & \equiv & 5 & \pmod 8 \end{cases}$$

**Exercice 16** *Trouver les deux derniers chiffres de $39^{39^{39}}$. Même question avec $17^{17^{17}}$.*

**Exercice 17** *Montrer que si $n$ est impair alors $n \mid 2^{n!} - 1$.*

**Exercice 18** *Soit $n$ un entier positif ou nul.*

1. *Démontrer la formule de Legendre :*

$$v(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots \lfloor \frac{n}{p^k} \rfloor + \cdots$$

2. *Prouver que chacun des termes de la suite $\left( \lfloor \frac{n}{p^k} \rfloor \right)$ est le quotient de la division euclidienne du précédent par $p$.*

**Exercice 19** *Soit $n \geq 2$ un entier et $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ sa décomposition en produit de facteurs premiers, où $p_1 < p_2 < \ldots < p_k$.*

1. *Montrer que $k \leq \dfrac{\log n}{\log 2}$.*

2. *Pour $1 \leq i \leq k$, montrer que $p_i \geq i+1$.*
3. *En déduire que*

$$\varphi(n) \geq \frac{\log 2}{2} \frac{n}{\log n}.$$

**Exercice 20** *On rappelle qu'un nombre de Carmichael est un entier $m$* non premier *tel que pour tout entier $a$ premier avec $m$ on ait*

$$a^{m-1} \equiv 1 \pmod{m}.$$

*On ne peut pas donc pas prouver qu'un tel nombre n'est pas premier en exhibant un $a$ premier avec $m$ tel que $a^{m-1} \not\equiv 1 \pmod{m}$.*

*Démontrer que $n = 561$ est un nombre de Carmichael.*

**Exercice 21** *Soit $m$ entier tel que $6m+1$, $12m+1$, $18m+1$ soient premiers. Démontrer que $n = (6m+1)(12m+1)(18m+1)$ est un nombre de Carmichael.*

**Exercice 22** *Soit $n$ un entier tel que*

1. *$n$ est impair, sans facteurs carrés.*
2. *Pour tout diviseur premier $p$ de $n$, $p-1$ divise $n-1$.*

*Démontrer que $n$ est un nombre de Carmichael.*

**Exercice 23** *Dans cette exercice on démontre que la condition suffisante pour qu'un entier soit un nombre de Carmichael, démontrée dans l'exercice précédent, est aussi nécessaire. Soit donc $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ un nombre de Carmichael.*

1. *Soit $a$ un entier premier avec $n$. Prouver que son ordre dans $(\mathbb{Z}/n\mathbb{Z})^*$ est un diviseur de $n-1$.*
2. *Soit $p$ un diviseur premier impair de $n$ et $\alpha = v_p(n)$ la valuation de $n$ en $p$.*
   (a) *A l'aide du théorème des restes chinois prouver qu'il existe un entier $a$, premier avec $n$, dont l'ordre dans $(\mathbb{Z}/n\mathbb{Z})^*$ est $p^{\alpha-1}(p-1)$.*
   (b) *En déduire que $\alpha = 1$, que $p-1$ est un diviseur de $n-1$ et enfin que $n$ est impair.*
3. *Démontrer qu'une puissance de 2 n'est jamais un nombre de Carmichael.*
4. *Déduire des questions précédentes que*
   (a) *$n$ est impair, sans facteurs carrés.*
   (b) *Pour tout diviseur premier $p$ de $n$, $p-1$ divise $n-1$.*

**Université Claude Bernard Lyon 1** **Master MAIM (1ère année)**
**Arithmétique et combinatoire** **Année 2011-12**

---

# Feuille 2 :
# Racines primitives

---

**Exercice 1** *Les nombres suivants possèdent-t-ils des racines primitives :*

1. $m = 23$ *?*
2. $m = 41$ *?*

*Si oui, en exhiber une.*

**Exercice 2** *Montrer que* 2 *est une racine primitive de* 101.

**Exercice 3** *Quel est l'ordre de* $3 \bmod 101$ *? Est-ce que* 3 *est une racine primitive de* 101 *?*

**Exercice 4** *(a) Prouver que* 2 *est une racine primitive de* 53.

*(b) Trouver toutes les solutions de*

$$2^x \equiv 22 \,(\mathrm{mod}\, 53).$$

**Exercice 5** *Soit* $p$ *un nombre premier impair et* $g$ *une racine primitive de* $p$.

*(i) Montrer que* $g^{(p-1)/2} \equiv -1 \,(\mathrm{mod}\, p)$.

*(ii) Montrer que* $(p-1)! \equiv g^{(p-2)(p-1)/2} \pmod p$.

*(iii) Retrouver le théorème de Wilson (voir exercice* **??***).*

**Exercice 6** *(a) Montrer que pour tout entier* $k \in \mathbb{N}$*, on a*

$$5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}.$$

*(b) En déduire que l'élément* $5 \bmod 2^m$ *est d'ordre* $2^{m-2}$ *dans* $(\mathbb{Z}/2^m\mathbb{Z})^*$.

*(c) Soit* $m \geq 3$ *et soit*

$$\begin{array}{rccl} \psi : & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & (\mathbb{Z}/2^m\mathbb{Z})^* \\ & (p, q) & \longmapsto & (-1)^p 5^q \bmod 2^m. \end{array}$$

*(i) Montrer que* $\psi$ *est un morphisme de groupes tel que* $\ker \psi = 2\mathbb{Z} \times 2^{m-2}\mathbb{Z}$.

*(ii) En déduire que* $(\mathbb{Z}/2^m\mathbb{Z})^*$ *est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

**Exercice 7** *Soit* $p = 7$ *et* $g = 3$.

*(a) Montrer que* $g$ *est un générateur de* $(\mathbb{Z}/p\mathbb{Z})^*$.

*(b) Calculer* $\log_g a$*, pour tout* $a$ *tel que* $1 \leq a \leq 6$.

*(c) Calculer* $\log_g 30$.

**Exercice 8 (Théorème de Lucas)** *Soient* $q, a$ *deux entiers naturels* $> 1$ *tels que*

1. $a^{q-1} \equiv 1 \bmod q$.
2. *Pour tout diviseur premier* $p$ *de* $q-1$, $a^{\frac{q-1}{p}} \not\equiv 1 \bmod q$.

*Démontrer que $q$ est premier et, de plus $a$ est un générateur de $\mathbf{F}_q$ (indication : considérer l'ordre de $a$ dans $\mathbf{F}_q$).*

**Exercice 9** *Etant donné un nombre premier $p$ et $x$ un nombre premier avec $p$, on notera $O_p(x)$ l'ordre de $x$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer que si $p$ est premier, $(a,p)=1$, et $4$ divise $O_p(a)$, alors $O_p(a)=O_p(-a)$. En déduire que si $p$ est un nombre premier de la forme $4k+1$, et $a$ un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ alors $-a$ est aussi un générateur.*

**Exercice 10** *Si $p=2q+1$ est premier, avec $q$ premier impair, et $a$ est un entier tel que $a^3-a \not\equiv 0 \bmod p$, montrer que $a$ ou bien $-a$ est un générateur multiplicatif modulo $p$.*

**Université Claude Bernard Lyon 1** **Master MAIM (1ère année)**
**Arithmétique et combinatoire** **Année 2011-12**

---

# Feuille 3 :
# Résidus quadratiques

---

**Exercice 1** Soit $p$ un nombre premier impair. Déterminer $\left(\frac{\frac{p+1}{2}}{p}\right)$ et $\left(\frac{\frac{p-1}{2}}{p}\right)$.

**Exercice 2**

1. Déterminer les $p$ premiers pour lesquels l'équation $x^2 \equiv 3 \pmod{p}$ admet au moins une solution ?
2. Pour quels $p$ premiers l'équation $x^2 \equiv 5 \pmod{p}$ a-t-elle des solutions ?

**Exercice 3** 131 et 263 sont premiers. Calculer $O_{263}(131)$ avec un minimum de calculs.

**Exercice 4** Montrer que les diviseurs premiers de $4n^2+1$ sont de la forme $4k+1$.

**Exercice 5** Résoudre l'équation $x^2 + 3x + 7 \equiv 0 \pmod{115}$.

**Exercice 6 (La méthode de Hensel)** Soit $p$ un nombre premier impair, $n \geq 1$ et $a \in \mathbb{Z}$ tel que $(a,p) = 1$.

(a) Montrer que $\bar{a} \in (\mathbb{Z}/p^n\mathbb{Z})^*$.

(b) On suppose que $x_1^2 \equiv a \pmod{p}$. Montrer que, pour tout entier $n \geq 1$, il existe un entier $x_n$, unique modulo $p^n$, qui vérifie

$$x_n \equiv x_1 \pmod{p}, \quad x_n^2 \equiv a \pmod{p^n}.$$

**Indication :** les $x_n$ se construisent par récurrence, en cherchant $x_{n+1}$ sous la forme

$$x_{n+1} = x_n + p^n u,$$

où $u$ est un nombre entier à déterminer.

(c) En déduire que la congruence $x^2 \equiv a \pmod{p^n}$ admet des solutions si et seulement si $\left(\frac{a}{p}\right) = 1$, et dans ce cas, elle admet exactement deux solutions modulo $p^n$.

(d) **Application :** résoudre $x^2 + x + 3 \equiv 0 \pmod{125}$.

**Exercice 7 (Résolution de $x^2 \equiv a \pmod{2^n}$ ($a$ impair))**

1. Soit $n \geq 3$, $a$ un entier impair. Démontrer que si la congruence $x^2 \equiv a \pmod{2^n}$ a des solutions, alors $a \equiv 1 \pmod{8}$.
2. On suppose $a \equiv 1 \pmod{8}$. Démontrer que $x^2 \equiv a \pmod{8}$ admet exactement 4 solutions modulo 8.
3. Supposons que $a \equiv 1 \pmod{8}$ et supposons qu'il existe un entier $x$ tel que $x^2 \equiv a \pmod{2^n}$.
   (a) Montrer que $a$ est un carré modulo $2^{n+1}$.
   **Indication :** on pourra calculer pour $y \in \mathbb{N}$, $(x + y2^{n-1})^2$.

(b) En déduire que $a$ possède au moins 4 racines carrés modulo $2^{n+1}$.

4. Conclure par récurrence que, pour tout $n \geq 3$, si $a \equiv 1 \pmod 8$, alors $a$ possède exactement 4 racines carrées modulo $2^n$.
**Indication :** on pourra considérer $C_n = \{x \in (\mathbb{Z}/2^n\mathbb{Z})^* : x \equiv 1 \pmod 8\}$ et

$$\begin{array}{rccc} \varphi : & (\mathbb{Z}/2^n\mathbb{Z})^* & \longrightarrow & C_n \\ & x & \longmapsto & x^2. \end{array}$$

**Exercice 8** On s'intéresse à l'équation $x^2 + x + 1 \equiv 0 \pmod n$.

1. Soit $S(n)$ la fonction arithmétique qui associe à l'entier $n \geq 1$ le nombre de solutions modulo $n$ de l'équation $x^2 + x + 1 \equiv 0 \pmod n$. Démontrer que la fonction $S$ est une *fonction arithmétique multiplicative* c'est à dire que $S(mn) = S(m)S(n)$ chaque fois que $m$ et $n$ sont premiers entre eux.
2. Pour quels $p$ premiers l'équation $x^2+x+1 = 0 \pmod p$ a-t-elle des solutions, c'est à dire tels que $S(p) > 0$.
3. Pour chacun de ces nombres premiers, discuter selon la valeur de $\alpha \geq 1$ la valeur de $S(p^\alpha)$.
4. Quels sont les entiers $n$ pour lesquels $x^2+x+1 \equiv 0 \pmod n$ a des solutions ?
5. Quel est le nombre de solutions de

$$x^2 + x + 1 \equiv 0 \pmod{2457}.$$

**Exercice 9**

1. Pour quels $p$ premiers l'équation $x^2+6x+1 = 0 \pmod p$ a-t-elle des solutions ?
2. Pour chacun de ces nombres premiers, discuter selon la valeur de $\alpha \geq 1$ le nombre de solutions de

$$x^2 + 6x + 1 \equiv 0 \pmod{p^\alpha}$$

3. Quels sont les entiers $n$ pour lesquels $x^2+6x+1 \equiv 0 \pmod n$ a des solutions ?

**Exercice 10** On appelle $n^{\text{ième}}$ nombre de Fermat le nombre $2^{2^n} + 1$.

1. Montrer que si un nombre premier est de la forme $2^k+1$ alors c'est un nombre de Fermat.
2. Soit $F_n = 2^{2^n} + 1$ un nombre de Fermat. Montrer que les diviseurs premiers de $F_n$ sont tous de la forme $k2^{n+1} + 1$ (si $p$ est un diviseur premier de $F_n$, on considèrera l'ordre de 2 modulo $p$ et on montrera qu'il est exactement $2^{n+1}$).
3. En considérant le caractére quadratique de 2 modulo $p$ montrer qu'on a un peu mieux : les diviseurs premiers de $F_n$ sont tous de la forme $k2^{n+2} + 1$.
4. En marchant sur les traces d'Euler, en déduire que $F_5 = 2^{32}+1 = 4294967297$ n'est pas premier.

**Exercice 11** Soit $p = F_n = 2^{2^n} + 1$, avec $n \geq 1$.

1. On suppose que $p$ est premier.
   (a) Montrer que $g$ est un générateur $(\mathbb{Z}/p\mathbb{Z})^*$ si et seulement si $\left(\frac{g}{p}\right) = -1$.
   (b) Montrer que 3 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.
2. Ici on ne suppose pas $p$ premier, mais seulement que

$$3^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Montrer que $p$ est premier. Ce test de primalité pour les nombres de Fermat est le test de Pepin.

**Exercice 12 (Calcul d'une racine carrée modulo $p$)** On donne dans cet exercice un algorithme efficace de calcul des racines carrées de $a$ dans $\mathbb{Z}/p\mathbb{Z}$ lorsque $p$ est premier impair.

1. Dans la cas ou $p \equiv 3 \pmod 4$ cet algorithme est particulièrement simple. Soit $a$ un carré modulo $p$. Démontrer que $a^{\frac{p+1}{4}}$ est un racine carrée de $a$.
2. A partir de maintenant $p$ est un nombre premier impair quelconque. Expliquer comment, en pratique, on peut trouver rapidement un entier $b$ qui ne soit pas un carré modulo $p$. On choisit un tel entier. On considère alors l'ensemble $E$ des couples $(e_1, e_2)$ satisfaisant
$$a^{e_1} b^{e_2} \equiv 1 \bmod p. \tag{1}$$
3. Montrer que $\left(\frac{p-1}{2}, 0\right) \in E$
4. Montrer que si $(e_1, e_2) \in E$ alors $e_2$ est pair.
5. Montrer que si $(e_1, e_2) \in E$ et si $e_1$ est impair alors
$$x = a^{\frac{e_1+1}{2}} b^{\frac{e_2}{2}}$$
est une racine carrée de $a$ modulo $p$.
6. Soit $(e_1, e_2) \in E$ avec $e_1$ pair. Soit $u = a^{\frac{e_1}{2}} b^{\frac{e_2}{2}}$. Que pouvez vous dire de $u^2$ ? En déduire un couple $(e'_1, e'_2) \in E$ avec $e'_1 = e_1/2$.
7. En déduire un algorithme de calcul d'une racine carrée de $a$ modulo $p$. Analyser la complexité de cet algorithme dans le pire des cas, c'est-à-dire le nombre maximum d'opérations à effectuer pour obtenir ainsi une racine carrée de $a$. Que se passe-t-il lorsque $p$ est de la forme $p = 4k + 3$ ?.

---

# Feuille 4 :
# Géométrie des nombres et applications

---

**Exercice 1** *Le but de cet exercice est de retrouver via une méthode connue sous le nom de* **descente infinie**, *le théorème d'Euler suivant :*

si $p$ est un nombre premier congru à $1 \bmod 4$, alors $p$ peut s'écrire comme la somme de deux carrés.

*On suppose donc que* $p \equiv 1 \pmod 4$.

*(a) Montrer qu'il existe un entier* $x_0 \in \mathbb{Z}$ *tel que* $-\frac{p}{2} < x_0 \leq \frac{p}{2}$ *et* $0 < \ell < p$ *tel que* $x_0^2 + 1 = \ell p$.

*(b) Soit* $m$ *le plus petit entier naturel (non nul) tel que* $mp$ *puisse s'écrire comme somme de deux carrés*

$$mp = x_1^2 + y_1^2.$$

*Si* $m = 1$, *le théorème est démontré. Supposons donc que* $m > 1$. *On a donc* $1 < m \leq \ell < p$. *Choisissons* $x_2, y_2 \in (-\frac{m}{2}, \frac{m}{2})$ *tels que*

$$x_2 \equiv x_1 \pmod m \quad \textit{et} \quad y_2 \equiv y_1 \pmod m.$$

*(i) Montrer qu'il existe* $0 \leq r < m$ *tel que* $x_2^2 + y_2^2 = rm$.

*(ii) Montrer que* $r \neq 0$ *(on pourra raisonner par l'absurde).*

*(iii) Montrer que*

$$x_1 y_2 - x_2 y_1 \equiv 0 \pmod m \quad \textit{et} \quad x_1 x_2 + y_1 y_2 \equiv 0 \pmod m$$

*(iv) En déduire qu'il existe* $x_3, y_3 \in \mathbb{Z}$ *tels que* $x_3^2 + y_3^2 = rp$.

*(v) Conclure.*

**Exercice 2** *Le but de cet exercice est de retrouver via la méthode de la descente infinie le théorème de Girard, Fermat, Lagrange suivant :*

tout entier naturel peut s'écrire comme la somme de 4 carrés.

*Comme on l'a vu dans la première étape de la preuve du théorème 4.4.3, on peut supposer que l'entier* $n = p$ *est un nombre premier.*

*(a) Si* $p \equiv 1 \bmod 4$, *prouver le résultat.*

*(b) On suppose maintenant dans toute la suite que* $p \equiv 3 \bmod 4$. *Soit* $z$ *le plus petit entier positif qui est un non résidu quadratique modulo* $p$.

*(i) Vérifier que* $z \geq 2$ *et que* $z - 1$ *est un résidu quadratique.*

*(ii) Montrer que* $-z$ *est un résidu quadratique modulo* $p$.

*(iii) Montrer qu'il existe* $x_0, y_0, m_0 \in \mathbb{Z}$ *tels que* $x_0^2 + y_0^2 + 1 = m_0 p$ *et* $|x_0| < \frac{p}{2}$, $|y_0| < \frac{p}{2}$ *et* $1 \leq m_0 < p$.

*(c) Soit* $m$ *le plus petit entier naturel (non nul) tel que* $mp$ *puisse s'écrire comme la somme de* 4 *carrés. Si* $m = 1$, *le théorème est démontré. Supposons donc que* $m > 1$ *et* $mp = a^2 + b^2 + c^2 + d^2$. *Choisissons* $A, B, C, D \in (-\frac{m}{2}, \frac{m}{2}]$ *tels que*

$$a \equiv A \pmod m, \quad b \equiv B \pmod m, \quad c \equiv C \pmod m \quad \textit{et} \quad d \equiv D \pmod m.$$

(i) *Montrer qu'il existe* $0 \leq r \leq m$ *tel que*

$$A^2 + B^2 + C^2 + D^2 = rm.$$

(ii) *Montrer que* $r \neq 0$ *et* $r \neq m$ *(on pourra raisonner par l'absurde).*

(iii) *Montrer qu'il existe* $\alpha, \beta, \gamma, \delta \equiv 0 \,(\mathrm{mod}\, m)$ *tels que*

$$(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2.$$

(iv) *Montrer que* $rp$ *peut s'écrire comme la somme de* 4 *carrés et conclure.*

**Exercice 3** *Le but de cet exercice est de donner une troisième démonstration du théorème d'Euler à travers la théorie des anneaux et plus particulièrement de* $\mathbb{Z}[i]$. *Rappelons que* $\mathbb{Z}[i]$ *est défini comme le sous-anneau de* $\mathbb{C}$ *formé des nombres complexes* $a + ib$, $a, b \in \mathbb{Z}$.

(a) *Soit* $N(a + ib) = a^2 + b^2$ *la norme de l'élément* $a + ib \in \mathbb{Z}[i]$.

(i) *Montrer que* $N(xy) = N(x)N(y)$, *pour tous* $x, y \in \mathbb{Z}[i]$.

(ii) *En déduire que* $x$ *est inversible dans* $\mathbb{Z}[i]$ *si et seulement si* $N(x) = 1$.

(iii) *En déduire que l'ensemble des éléments inversibles de* $\mathbb{Z}[i]$ *est*

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$

(b) *Montrer que* $\mathbb{Z}[i]$ *est euclidien donc principal.*
Indication : *on pourra montrer que si* $x, y \in \mathbb{Z}[i]$, *alors*
- *si* $x$ *divise* $y$, *on a* $N(x) \leq N(y)$.
- *si* $x$ *ne divise pas* $y$, *alors il existe* $q$ *et* $r \in \mathbb{Z}[i]$ *tels que*

$$y = qx + r \quad \textit{avec } N(r) < N(x).$$

(c) *Soit* $p$ *un nombre premier tel que* $p \equiv 1 \bmod 4$. *On sait qu'il existe* $a \in \mathbb{Z}$ *tel que* $a^2 \equiv -1 \bmod p$.

(i) *Montrer que l'élément* $p$ *n'est pas premier dans* $\mathbb{Z}[i]$. *Donc il n'est pas irréductible et il existe* $\alpha, \beta \in \mathbb{Z}[i]$ *non inversibles tels que* $p = \alpha\beta$.

(ii) *En déduire que* $N(\alpha) = p$, *puis que* $p$ *s'écrit comme la somme de deux carrés.*

**Exercice 4** *Pour tout entier naturel* $n \geq 1$ *on note* $r_3(n)$ *le nombre de triplets* $(x_1, x_2, x_3) \in \mathbb{Z}^3$ *tels que*

$$n = x_1^2 + x_2^2 + x_3^2.$$

1. *Démontrer que si* $n \equiv 7 \pmod 8$, $r_3(n) = 0$.
2. *Démontrer que* $r_3(4n) = r_3(n)$.
3. *En déduire que si* $n = 4^a(8b+7)$ *où* $a \in \mathbb{N}$, $b \in \mathbb{N}$, *alors* $n$ *n'est pas une somme de 3 carrés.*

*Gauss a démontré la réciproque : tout entier naturel* $n$ *qui n'est pas de la forme* $n = 4^a(8b + 7)$ *est une somme de* 3 *carrés.*

# Feuille 5 : Autour de la répartition des nombres premiers : approches élémentaires.

**Exercice 1** Dans cet exercice, on admettra le théorème des nombres premiers, c'est à dire que $\pi(x) \sim x/\ln x$, $x \to +\infty$. On note $p_n$ le $n$-ième nombre premier. Montrer que $p_n \sim n \ln n$, $n \to +\infty$.

**Exercice 2** Soit $P^+(n)$ le plus grand facteur premier d'un entier $n$. Calculer

$$\sum_{P^+(n)\leq 5} \frac{1}{n}.$$

**Exercice 3 (Postulat de Bertrand)** En partant de l'encadrement

$$\forall x \geq 30, \qquad 0.9 \, \frac{x}{\log x} \leq \pi(x) \leq 1.2 \, \frac{x}{\log x},$$

prouver que pour tout $n \geq 30$, il existe un nombre premier strictement compris entre $n$ et $2n$. En déduire le résultat [1] suivant :

$$\forall n \geq 2, \text{il existe un nombre premier } p \text{ satisfaisant } n < p < 2n.$$

**Exercice 4** Montrer que, pour $n > 1$, $n!$ n'est pas de la forme $a^b$ avec $b > 1$.
*Indication :* on considérera le plus grand premier $p \leq n$ et on utilisera le théorème de Bertrand.

**Exercice 5** Soit $x$ un réel, $x > 1$. Démontrez les estimations suivantes :

$$(a) \ \ln x \leq \sum_{d\leq x} \frac{1}{d} \leq 1 + \ln x \qquad (b) \ \sum_{d>x} \frac{1}{d^2} \leq \frac{1}{x-1}.$$

**Exercice 6** Pour $n \geq 1$, on note $d(n)$ le nombre de diviseur de l'entier $n$,

$$d(n) = \sum_{d|n} 1.$$

Montrer que

$$\frac{1}{x} \sum_{n\leq x} d(n) = \ln x + O(1).$$

**Exercice 7** En utilisant la méthode dite de *l'hyperbole de Dirichlet*, le but de l'exercice est d'améliorer l'estimation démontrée dans l'exercice précédent.

(a) Montrer que $\sum_{n\leq x} d(n)$ est le nombre de points à coordonnées entières situés dans le quart de plan $u \geq 1$, $v \geq 1$ et sous l'hyperbole d'équation $uv = x$.

1. Remarquons une conjecture analogue due à Legendre : pour tout entier $n \geq 1$, il existe un nombre premier entre $n^2$ et $(n+1)^2$. En 2012, on ne sait toujours pas si cette conjecture est vraie ou non.

(b) En utilisant la symétrie du graphe de l'hyperbole $uv = x$, en déduire que

$$\sum_{n\leq x} d(n) = 2\sum_{d\leq\sqrt{x}} \left\lfloor \frac{x}{d} \right\rfloor - \lfloor\sqrt{x}\rfloor^2.$$

(c) En utilisant la formule d'Abel, retrouver le résultat bien connu suivant :

$$\sum_{n\leq x} \frac{1}{n} = \ln x + \gamma + O\left(\frac{1}{x}\right),$$

où $\gamma$ est la constante définie par

$$\gamma = 1 - \int_1^{+\infty} \frac{\{t\}}{t^2}\, dt.$$

(d) En déduire que

$$\frac{1}{x}\sum_{n\leq x} d(n) = \ln x + (2\gamma - 1) + O\left(\frac{1}{\sqrt{x}}\right).$$

**Exercice 8** On note $p_n$ le $n$-ième nombre premier.

(a) Sans utiliser le théorème des nombres premiers, montrer que la série

$$\sum_n \frac{1}{p_n \ln p_n}$$

converge.

(b) En utilisant le théorème des nombres premiers, donner un équivalent du reste

$$R_n := \sum_{k=n+1}^{+\infty} \frac{1}{p_k \ln p_k}$$

**Exercice 9** (a) Montrer que si $f : [2, +\infty[ \longrightarrow \mathbb{R}$ est une fonction de classe $C^1$, alors

$$\sum_{p\leq x} f(p) = \pi(x)f(x) - \int_2^x f'(t)\pi(t)\, dt.$$

(b) On admet dans cette question que

$$\pi(x) = \frac{x}{\ln x} + O\left(\frac{x}{(\ln x)^2}\right), \qquad x \geq 2.$$

Retrouver alors le fait qu'il existe une constante $C > 0$ telle que

$$\sum_{p\leq x} \frac{1}{p} = \ln\ln x + C + O\left(1/\ln x\right)$$

**Exercice 10**

1. Montrer que

$$\lim_{x\to+\infty} \sum_{\sqrt{x}<p\leq x} \frac{1}{p} = \ln 2.$$

2. Notons pour un entier $n$, $P^+(n)$ le plus grand facteur premier de $n$ et posons

$$A_x = \left\{n \leq x : P^+(n) > \sqrt{n}\right\}.$$

(i) Montrer que $n \in A_x$ si et seulement s'il existe un nombre premier $p$ et un entier $q$ tel que $n = pq$ et $q < p \leq \frac{x}{q}$. Montrer de plus qu'un telle décomposition est unique.

(ii) Montrer que

$$\mathrm{card}(A_x) = \sum_{p \leq \sqrt{x}} (p-1) + \sum_{\sqrt{x} < p \leq x} \left\lfloor \frac{x}{p} \right\rfloor .$$

3. En déduire, que lorsque $x \to +\infty$, une proportion positive des entiers $n \leq x$ ont leur plus grand facteur premier $> \sqrt{n}$.

**Exercice 11** Le but de l'exercice est d'évaluer

$$\sum_{pq \leq x} \frac{1}{pq}$$

où $p$ et $q$ désignent des nombres premiers.

1. Montrer qu'il existe une constante $C$ telle que

$$\sum_{pq \leq x} \frac{1}{pq} = (\ln\ln x + C) \sum_{p \leq \frac{x}{2}} \frac{1}{p} + O\left( \sum_{p \leq \frac{x}{2}} \frac{1}{p} \ln\left( \frac{\ln x}{\ln(x/p)} \right) \right).$$

2. En déduire que

$$\sum_{pq \leq x} \frac{1}{pq} = (\ln\ln x)^2 + 2C \ln\ln x + O\left( 1 + \sum_{p \leq \frac{x}{2}} \frac{1}{p} \ln\left( \frac{\ln x}{\ln(x/p)} \right) \right).$$

3. Montrer que

$$\sum_{p \leq \frac{x}{2}} \frac{1}{p} \ln\left( \frac{\ln x}{\ln(x/p)} \right) \leq \int_1^{\ln x / \ln 2} \sum_{x^{\frac{v-1}{v}} < p \leq x/2} \frac{1}{p} \frac{dv}{v}.$$

4. En utilisant que $\int_1^{+\infty} \ln\left(\frac{v}{v-1}\right) \frac{dv}{v}$ converge, en déduire que

$$\sum_{p \leq \frac{x}{2}} \frac{1}{p} \ln\left( \frac{\ln x}{\ln(x/p)} \right) = O(1).$$

5. En déduire que

$$\sum_{pq \leq x} \frac{1}{pq} = (\ln\ln x)^2 + 2C \ln\ln x + O(1).$$

---

# Feuille 6 :
# Fonctions arithmétiques.

---

Dans toute cette fiche :

1. $\mu$ représente la fonction de Möbius.
2. $\varphi$ la fonction d'Euler : $\varphi(n) = \sum_{\substack{1\leq m\leq n\\(m,n)=1}} 1$.
3. $d(n) = \sum_{d|n} 1$ le nombre des diviseurs de l'entier $n$.
4. $\sigma(n) = \sum_{d|n} d$ la somme des diviseurs de l'entier $n$.

---

**Exercice 1** Déterminer toutes les fonctions arithmétiques $f$ complètement multiplicatives telles que $F = \mathbf{I} * f$ soit encore complètement multiplicative.

**Exercice 2** Montrer que la fonction arithmétique $f$ définie par $f(n) = (-1)^{n+1}$ pour $n \geq 1$ est multiplicative. Soit $g$ l'inverse de $f$ pour la convolution. Expliciter $g(p^\alpha)$ pour $p$ premier et $\alpha \in \mathbb{N}$ puis $g(n)$ pour un entier $n \geq 1$ quelconque.

**Exercice 3** On désigne par $\Omega(n)$ le nombre de facteurs premiers de $n$, *comptés avec leur ordre de multiplicité* c'est-à-dire

$$\Omega(n) = \sum_{i=1}^{k} \alpha_i, \text{ où } n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

est la décomposition en facteurs premiers de $n$. La *fonction $\lambda$ de Liouville* est définie par $\lambda(n) = (-1)^{\Omega(n)}$. Montrer que $\lambda$ est complètement multiplicative, et que le produit de convolution $\lambda * \mathbf{I}$ est la fonction caractéristique des carrés c'est-à-dire que

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{si } n \text{ est un carré} \\ 0 & \text{si } n \text{ n'est pas un carré.} \end{cases}$$

**Exercice 4**

1. Montrer que pour tout $n > 1$ on a $\varphi(n)\sigma(n) < n^2$.
2. Montrer que pour tout $n > 1$ on a $\varphi(n)d(n) \geq n$ avec égalité si et seulement si $n = 2$.

**Exercice 5** On dit qu'un entier $n$ est **abondant** si $\sigma(n) \geq 2n$. Montrer que si $n$ est abondant et impair il admet au moins 3 facteurs premiers.

**Exercice 6**

1. Montrer que $\varphi(mn) \geq \varphi(m)\varphi(n)$, avec égalité seulement si $(m, n) = 1$.
2. Montrer que $d(mn) \leq d(m)d(n)$ avec égalité si et seulement si $(m, n) = 1$.

**Exercice 7** La fonction $d$ prend elle plus souvent des valeurs paires ou impaires ?

**Exercice 8** Montrer que pour tout $n$, $\sigma(3n-1)$ est un multiple de 3.

**Exercice 9** Soient $F : [1, +\infty[ \longrightarrow \mathbb{C}$ et

$$G(x) = \sum_{n \leq x} F\left(\frac{x}{n}\right).$$

Montrer que

$$F(x) = \sum_{n \leq x} \mu(n) G\left(\frac{x}{n}\right).$$

Cette formule est connue sous le nom de *deuxième formule d'inversion de Möbius.*

**Exercice 10** Soit $x$ un réel $x \geq 1$.

1. Montrer, par exemple en utilisant la deuxième formule d'inversion de Möbius (voir exercice précédent), que

$$\sum_{n \leq x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1.$$

2. En déduire que

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1.$$

**Exercice 11**

1. Montrer que $\mu * N_1 = \varphi$.
2. En déduire que, pour tout $n \geq 1$, on a

$$n = \sum_{d|n} \varphi(d).$$

3. Montrer que

$$\sigma(n) = \sum_{k|n} d(k) \varphi\left(\frac{n}{k}\right).$$

**Exercice 12** Montrer que

$$\frac{1}{x} \sum_{n \leq x} \frac{\sigma(n)}{n} = \frac{\pi^2}{6} + O\left(\frac{\log x}{x}\right).$$

**Exercice 13** On définit la *fonction de von Mangoldt* $\Lambda(n)$ par

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^k \text{ est une puissance d'un nombre premier,} \\ 0 & \text{sinon.} \end{cases}$$

Remarquons alors que si $\psi$ désigne la fonction de Chebyshev, on a

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

1. Montrer que

$$\sum_{d|n} \Lambda(d) = \log n.$$

2. Montrer que pour $x \geq 2$, on a

$$\sum_{m \leq x} \psi\left(\frac{x}{m}\right) = \sum_{d \leq x} \Lambda(d) \left\lfloor \frac{x}{d} \right\rfloor .$$

3. Montrer que

$$\sum_{m \leq x} \psi\left(\frac{x}{m}\right) = x \log x - x + O(\log x).$$

4. Montrer que

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1).$$

5. En déduire une nouvelle preuve de la formule de Mertens :

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1).$$

# Feuille 7 :
# Séries de Dirichlet

Dans toute cette fiche :

1. $\mu$ représente la fonction de Möbius.
2. $\varphi$ la fonction d'Euler : $\varphi(n) = \sum_{\substack{1\leq m\leq n\\(m,n)=1}} 1$.
3. $d(n) = \sum_{d|n} 1$ le nombre des diviseurs de l'entier $n$.
4. $\sigma(n) = \sum_{d|n} d$ la somme des diviseurs de l'entier $n$.

---

**Exercice 1** Déterminer les abscisses de convergence et de convergence absolue de

1. $\displaystyle\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$.
2. $\displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ avec $a_n = \begin{cases} 1 & \text{si } n \text{ est un carré} \\ 0 & \text{sinon.} \end{cases}$

**Exercice 2** Soit $\sum_n a_n n^{-s}$ une série de Dirichlet. Supposons que la suite des coefficients $(a_n)_n$ soit bornée. Montrer alors que l'abscisse de convergence absolue $\sigma_a$ vérifie $\sigma_a \leq 1$. Est-ce que cette borne est optimale ?

**Exercice 3** Soit $\sum_n a_n n^{-s}$ une série de Dirichlet et supposons que la suite des sommes partielles $\displaystyle\sum_{k=1}^{N} a_k$ soit bornée. Montrer alors que $\sigma_c \leq 0$.

**Exercice 4** Soit $\sum_n a_n n^{-s}$ une série de Dirichlet telle que $a_n \geq 0$, $n \geq 1$. Supposons que la série converge sur $\Re(s) > \sigma_0$ pour un certain $\sigma_0 \in \mathbb{R}$ et notons

$$F(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}, \qquad \Re(s) > \sigma_0.$$

Montrer que si $F$ se prolonge analytiquement au voisinage de $\sigma_0$, alors $\sigma_c < \sigma_0$.

**Exercice 5** Soit $\lambda$ la fonction de Liouville définie dans la feuille précédente. Déterminer l'abscisse de convergence absolue de

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s}.$$

Transformer la somme en un produit eulérien et montrer que pour $\Re(s) > 1$ on a

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)}.$$

**Exercice 6**

1. Montrer que la fonction $d$ est le produit de convolution d'une fonction très simple par elle même.
2. En utilisant le théorème relatif à la série de Dirichlet d'un produit de convolution démontrer que l'abscisse de convergence de la série de Dirichlet

$$\sum_{n=1}^{\infty} \frac{d(n)}{n^s}$$

est inférieure ou égale à 1 et que, pour $\Re(s) > 1$ la somme de cette série de Dirichlet est $\zeta(s)^2$.

**Exercice 7** Démontrer que pour tout $s$, $\Re(s) > 2$, on a

$$\sum_{n\geq 1} \frac{\sigma(n)}{n^s} = \zeta(s)\zeta(s-1)$$

Démontrer que l'abscisse de convergence de cette série de Dirichlet est exactement2.

**Exercice 8**

1. Démontrer que, pour $\Re(s) > 2$ la série génératrice de $\varphi(n)$ est absolument convergente et que

$$\sum_{n\geq 1} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$$

2. Retrouver ce résultat plus rapidement, en partant de l'identité

$$n = \sum_{d|n} \varphi(d),$$

que vous exprimerez comme une identité de convolution.

3. En utilisant la minoration $\varphi(n) \geq \dfrac{\log 2}{2} \dfrac{n}{\log n}$ montrer que l'abscisse de convergence de cette série de Dirichlet est 2.

**Exercice 9** On se propose dans cet exercice de calculer un équivalent du nombre $S(x)$ des entiers sans facteur carré, inférieurs ou égaux à $x$.

1. Montrer que $S(x) = \sum_{n\leq x} \mu^2(n)$, où $\mu$ est la fonction de Möbius.
2. Montrer que la série de Dirichlet

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s}$$

converge pour $\Re(s) > 1$, et que, alors

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \frac{\zeta(s)}{\zeta(2s)}.$$

3. Montrer qu'il existe une unique fonction arithmétique multiplicative $g$ telle que $\mu^2 = \mathbf{I} * g$, et expliciter $g(p^\alpha)$. En déduire que $g(n) = 0$ si $n$ n'est pas un carré, et que $g(n^2) = \mu(n)$.

4. Montrer que la série de Dirichlet de $g$ converge absolument pour $\Re(s) > 1/2$, et que, dans ce cas
$$\sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \frac{1}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{2s}}.$$

5. Transformer la somme $\sum_{n\leq x} \mu^2(n)$ en utilisant l'égalité $\mu^2 = g * \mathbf{I}$, puis une permutation de l'ordre de sommation. En déduire que
$$S(x) = \frac{x}{\zeta(2)} + O(\sqrt{x}).$$

**Exercice 10** Soit $S := \{n \geq 1 \ : \ p|n \longrightarrow p^2|n\}$ et $S_x = \text{card}\,(S \cap [1, x])$.

1. Montrer que tout élément de $S$ s'écrit de manière unique sous la forme $m^3u^2$ avec $m$ sans facteur carré.
2. En déduire que
$$S_x = \sum_{m\leq \sqrt[3]{x}} \mu(m)^2 \left\lfloor \sqrt{\frac{x}{m^3}} \right\rfloor = \sqrt{x} \sum_{m=1}^{\infty} \frac{\mu(m)^2}{m^{3/2}} + O\left(x^{1/3}\right)$$

3. En transformant la somme ci-dessus en un produit eulérien, montrer que
$$S_x \sim \frac{\zeta(3/2)}{\zeta(3)} \sqrt{x}.$$

**Exercice 11** On peut démontrer relativement simplement, en utilisant le théorème des nombres premiers, que la série
$$\sum_{n=1}^{+\infty} \frac{\mu(n)}{n}$$
est convergente (et réciproquement, si l'on admet que cette série est convergente, il est assez facile de prouver le théorème des nombres premiers).

En considérant la série de Dirichlet
$$\sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}$$
démontrer que
$$\sum_{n=1}^{+\infty} \frac{\mu(n)}{n} = 0.$$

**Exercice 12** Soit $G$ la série de Dirichlet associée à la fonction de Möbius,
$$G(s) = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}.$$

1. Montrer que la série $G$ converge absolument sur $\Re(s) > 1$.
2. Montrer que $\zeta(s)G(s) = 1$, $\Re(s) > 1$.
3. En déduire que
$$\sum_{n\leq x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} + O\left(\frac{1}{x}\right).$$

**Exercice 13**

1. Montrer que, pour tout entier $n$, on a
$$\varphi(n) = \sum_{d'd=n} d'\mu(d).$$
2. Montrer que
$$\sum_{n\leq x} \varphi(n) = \frac{3x^2}{\pi^2} + O(x\log x).$$
3. En déduire que la probabilité que deux entiers naturels (positifs) soient premiers entre eux est de $\frac{6}{\pi^2}$.

**Université Claude Bernard Lyon 1** **Master MAIM (1ère année)**
**Arithmétique et combinatoire** **Année 2011-12**

Partiel du 30 mars 2012
Durée : 2h

---

Les documents ne sont pas autorisés. Le sujet comporte 4 exercices indépendants qui pourront être traités dans l'ordre de votre choix. Une attention particulière devra être apportée à la rédaction qui sera un élément important d'appréciation.

---

**Exercice 1**

(a) 13 est-il une racine primitive de 19 ?

(b) Soit $n$ un entier positif. Montrer que 19 divise $2^{3n+4} + 3^{2n+1}$ si et seulement si $8^n \equiv 9^n \pmod{19}$.

(c) Calculer l'inverse de 8 modulo 19.

(d) En déduire l'ensemble des entiers $n$ tels que 19 divise $2^{3n+4} + 3^{2n+1}$.

**Exercice 2** Soient $n$ un entier $\geq 2$ et $N = 5(n!)^2 - 1$.

(a) Montrer que tous les facteurs premiers de $N$ sont strictement plus grand que $n$.

(b) Montrer que $N$ possède un facteur premier $p$ tel que $p \not\equiv 1 \pmod{5}$.

(c) Montrer que $p$ est un résidu quadratique modulo 5 et en déduire que $p \equiv -1 \pmod{5}$.

(d) Montrer que l'ensemble des nombres premiers congrus à $-1$ modulo 5 est infini.

**Exercice 3**

(a) Soit $n$ un entier sans facteur carré, c'est-à-dire que si $p$ est un nombre premier qui divise $n$, alors $p^2$ ne divise pas $n$. Supposons qu'il existe trois entiers $a, b$ et $d$ tels que $n = a^2 + db^2$.

(i) Montrer que $n$ et $b$ sont premiers entre eux.

(ii) En déduire que $-d$ est un carré modulo $n$.

(b) Soit $d \geq 1$ un entier, $n$ un nombre entier strictement positif tel que $-d$ est un carré modulo $n$. Le but de cette question est de montrer que l'un au moins des nombres

$$n, 2n, 3n, \ldots, hn$$

est de la forme $a^2 + db^2$, où $h = \lfloor \frac{4\sqrt{d}}{\pi} \rfloor$.

(i) Soit

$$L = \{(a, b) \in \mathbb{Z}^2 : a \equiv ub \pmod{n}\}$$

où $u \in \mathbb{Z}$ vérifie $u^2 \equiv -d \pmod{n}$. Montrer que $L$ est un réseau de $\mathbb{R}^2$ et calculer son covolume.

(ii) Soit $r > 0$ et

$$C_d(r) = \{(x, y) \in \mathbb{R}^2 : x^2 + dy^2 \leq r\}.$$

Montrer que la surface de $C_d(r)$ est $\pi r/\sqrt{d}$.

(iii) En déduire qu'il existe $r > 0$ tel que l'intersection $L \cap C_d(r)$ contienne un élément non nul.

(iv) Conclure.

(c) Soit $p$ un nombre premier impair. Montrer que $p$ est de la forme $a^2 + 2b^2$ si et seulement si $p \equiv 1$ ou $3 \pmod 8$.

**Exercice 4** Soit $0 < a < 1$.

(a) Montrer qu'il existe une constante $\gamma(a) > 0$ telle que

$$\sum_{n \leq x} \frac{1}{n^a} = \frac{x^{1-a}}{1-a} - \gamma(a) + O(x^{-a}).$$

(b) Montrer que

$$\int_2^x \frac{dt}{t^a \log t} = \frac{x^{1-a}}{(1-a)\log x} + O\left(\frac{x^{1-a}}{(\log x)^2}\right).$$

(c) On admet dans cette question que

$$\pi(t) = \frac{t}{\log t} + O\left(\frac{t}{(\log t)^2}\right),$$

où on rappelle que $\pi(t)$ désigne le nombre de nombres premiers $\leq t$. Montrer que

$$\sum_{p \leq x} \frac{1}{p^a} = \frac{x^{1-a}}{(1-a)\log x} + O\left(\frac{x^{1-a}}{(\log x)^2}\right).$$

---

**Barème :** toutes les questions seront notées sur 1 point sauf les questions (c) de l'exercice 2, (biv) de l'exercice 3 et (a) de l'exercice 4 qui seront notées sur 2 points.

Exercice 1 : 4 pts.
Exercice 2 : 5 pts.
Exercice 3 : 8 pts.
Exercice 4 : 4 pts.

**Université Claude Bernard Lyon 1** **Master MAIM (1ère année)**
**Arithmétique et combinatoire** **Année 2011-12**

Partiel du 30 mars 2012
Correction.

---

**Exercice 1**

(a) Comme 19 est un nombre premier, on a $\varphi(19) = 19 - 1 = 18$. Ainsi 13 est une racine primitive de 19 si et seulement si l'ordre de 13 dans $(\mathbb{Z}/19\mathbb{Z})^*$ est 18. L'ordre de tout élément devant diviser $18 = 2 \times 3^2$, les seules possibilités sont 2, 3, 6, 9 ou 18. Il faut donc calculer $13^2$, $13^3$, $13^6$ et $13^9$. On a

$$\begin{aligned} 13^2 &= 169 \equiv 17 \equiv -2 \pmod{19} \\ 13^3 &= 13 \times 13^2 \equiv -26 \equiv 12 \pmod{19} \\ 13^6 &= (13^2)^3 \equiv -2^3 \equiv 11 \pmod{19} \\ 13^9 &= 13 \times (13^2)^4 \equiv 13 \times 2^4 \equiv 18 \equiv -1 \pmod{19}. \end{aligned}$$

Comme $13^2, 13^3, 13^6$ et $13^9$ ne sont pas congrus à 1 modulo 19, on en déduit que 13 est une racine primitive de 19.

(b) Remarquons que 19 divise $2^{3n+4} + 3^{2n+1}$ si et seulement si $2^{3n+4} + 3^{2n+1} \equiv 0 \pmod{19}$, c'est-à-dire

$$2^4 \times 8^n \equiv -3 \times 9^n \pmod{19}. \tag{1}$$

Or $2^4 = 16 \equiv -3 \pmod{19}$. Comme 16 et 19 sont premiers entre eux, 16 est inversible modulo 19 et l'équation (1) est équivalente à

$$8^n \equiv 9^n \pmod{19}.$$

(c) On applique l'algorithme d'Euclide qui donne les divisions successives

$$19 = 8 \times 2 + 3, \quad 8 = 3 \times 2 + 2, \quad 3 = 2 \times 1 + 1,$$

ce qui donne

$$1 = 3 - 1 \times 2 = 3 - (8 - 3 \times 2) = -8 + 3 \times 3 = -8 + 3(19 - 2 \times 8) = 3 \times 19 - 7 \times 8.$$

Ainsi, l'inverse de 8 modulo 19 est $-7 \equiv 12 \pmod{19}$.

(d) D'après les questions (b) et (c), 19 divise $2^{3n+4} + 3^{2n+1}$ si et seulement si $(9 \times 12)^n \equiv 1 \pmod{19}$. Or $9 \times 12 \equiv 13 \pmod{19}$. Ainsi on obtient que 19 divise $2^{3n+4} + 3^{2n+1}$ si et seulement si $13^n \equiv 1 \pmod{19}$. Comme 13 est une racine primitive de 19, on obtient que l'ensemble des entiers $n$ tels que 19 divise $2^{3n+4} + 3^{2n+1}$ est l'ensemble des multiples de 18.

**Exercice 2**

(a) On raisonne par l'absurde en supposant qu'il existe un facteur premier $p$ de $N$ qui est inférieur ou égal à $n$. Alors $p$ divise aussi $(n!)^2$ et donc $p$ divise $N - 5(n!)^2 = -1$, ce qui est absurde. Autrement dit, tous les facteurs premiers de $N$ sont strictement plus grand que $n$.

(b) On raisonne encore par l'absurde en supposant que tous les facteurs premiers $p$ de $N$ sont congrus à 1 modulo 5. Alors $N$ est lui aussi congru à 1 modulo 5, ce qui est absurde car

$$N = 5(n!)^2 - 1 \equiv -1 \pmod 5.$$

Ainsi il existe un facteur premier $p$ de $N$ tel que $p \not\equiv 1 \pmod 5$.

(c) Remarquons tout d'abord que $p \not\equiv 0 \pmod 5$, car sinon 5 diviserait $N$ et donc aussi $5(n!)^2 - N = 1$, ce qui n'est pas possible. D'autre part, d'après la première question, on a $p > n \geq 2$. En particulier, $p$ est un nombre premier impair. La loi de réciprocité quadratique implique alors que

$$\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)(-1)^{\frac{(p-1)(5-1)}{4}} = \left(\frac{5}{p}\right).$$

Comme $p$ divise $N$, on a $5(n!)^2 \equiv 1 \pmod p$, ce qui donne par périodicité et multiplicativité du symbole de Legendre que

$$1 = \left(\frac{1}{p}\right) = \left(\frac{5(n!)^2}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{(n!)^2}{p}\right) = \left(\frac{5}{p}\right).$$

Ainsi, on obtient que $\left(\frac{p}{5}\right) = 1$, ce qui signifie que $p$ est un résidu quadratique modulo 5.

Ce qui précède signifie que $p$ est un carré non nul modulo 5. Or, en dressant la table des carrés modulo 5, on voit que les seuls carrés (non nuls) modulo 5 sont $\pm 1 \pmod 5$. Or d'après la question (b), $p \not\equiv 1 \pmod 5$. Donc $p \equiv -1 \pmod 5$.

(d) Pour tout $n \geq 2$, la méthode précédente donne un nombre premier $p > n$ tel que $p \equiv -1 \pmod 5$. Ainsi par récurrence, on peut construire une infinité de nombres premiers $p$ congrus à $-1$ modulo 5.

**Exercice 3**

(a) (i) Raisonnons par l'absurde en supposant que $n$ et $b$ ne sont pas premiers entre eux. Alors il existe un nombre premier $p$ qui divise $n$ et $b$. Alors $p$ divise aussi $a^2 = n - db^2$. Nécessairement $p$ divise $a$ et donc $p^2$ divise $a^2$. Comme $p^2$ divise aussi $b^2$, on en déduit que $p^2$ divise $n$, ce qui est contraire à l'hypothèse que $n$ est sans facteur carré.

(ii) Comme $n$ et $b$ sont premiers entre eux, $b$ est inversible modulo $n$. Autrement dit, il existe un entier $c$ tel que $bc \equiv 1 \pmod n$. Comme $-db^2 \equiv a^2 \pmod n$, on en déduit que

$$-d \equiv (ac)^2 \pmod n,$$

ce qui prouve que $-d$ est un carré modulo $n$.

(b) (i) Considérons

$$\begin{array}{rccc} \psi : & \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & (a,b) & \longmapsto & (a - ub) \bmod n. \end{array}$$

On vérifie facilement que $\psi$ est un morphisme de groupes surjectifs et on a $\ker \psi = L$. Donc $\psi$ induit un isomorphisme entre $\mathbb{Z}^2/L$ et $\mathbb{Z}/n\mathbb{Z}$. On obtient ainsi que $L$ est un sous-groupe d'indice fini de $\mathbb{Z}^2$. Un théorème du cours implique alors que $L$ est un réseau de $\mathbb{R}^2$, de covolume

$$\mathrm{covol}(L) = [\mathbb{Z}^2 : L]\,\mathrm{covol}(\mathbb{Z}^2) = [\mathbb{Z}^2 : L].$$

Comme $\mathbb{Z}^2/L \simeq \mathbb{Z}/n\mathbb{Z}$, on a $[\mathbb{Z}^2 : L] = n$, d'où $\mathrm{covol}(L) = n$.

(ii) Considérons

$$\begin{array}{rccc} \varphi : & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \longmapsto & (u,v) = (x, \sqrt{d}\, y) \end{array}$$

et notons $D(0,\sqrt{r})$ le disque de centre 0 et de rayon $\sqrt{r}$. Il est clair que $\varphi$ réalise une bijection de $C_d(r)$ sur $D(0,\sqrt{r})$. La formule de changement de variable donne alors que

$$\int_{C_d(r)} dx\, dy = \int_{D(0,\sqrt{r})} |\mathrm{Jac}(\varphi^{-1})(u,v)|\, du\, dv.$$

Or il est immédiat de vérifier que $|\mathrm{Jac}(\varphi^{-1})(u,v)| = 1/\sqrt{d}$, ce qui donne

$$\int_{C_d(r)} dx\, dy = \frac{1}{\sqrt{d}} \int_{D(0,\sqrt{r})} du\, dv = \frac{\pi r}{\sqrt{d}}.$$

(iii) L'ensemble $C_d(r)$ est clairement un sous-ensemble convexe, symétrique et compact de $\mathbb{R}^2$. De plus, d'après la question précédente, sa mesure de Lebesgue est $\pi r/\sqrt{d}$. Le théorème de Minkowski implique alors que si

$$r \geq \frac{4\sqrt{d}\ \mathrm{covol}(L)}{\pi} = \frac{4\sqrt{d}\, n}{\pi}$$

alors $C_d(r) \cap L$ contient un vecteur non nul.

(iv) D'après la question précédente, il existe un vecteur $(a,b) \in C_d(\frac{4\sqrt{d}\, n}{\pi}) \cap L$, $(a,b) \neq (0,0)$. Cela signifie d'une part que $a^2 \equiv u^2 b^2 \pmod{n}$. Comme $u^2 \equiv -d \pmod{n}$, on obtient que $a^2 + db^2 \equiv 0 \pmod{n}$. Ainsi, il existe un entier relatif $k$ tel que $a^2 + db^2 = kn$. Comme $d$ et $n$ sont des entiers strictement positifs, nécessairement on a $k \geq 1$. D'autre part, comme $(a,b) \in C_d(\frac{4\sqrt{d}\, n}{\pi})$, on a aussi

$$kn = a^2 + db^2 \leq \frac{4\sqrt{d}\, n}{\pi},$$

soit $k \leq \frac{4\sqrt{d}}{\pi}$. Ainsi il existe un entier $k$, compris entre 1 et $h = \lfloor \frac{4\sqrt{d}}{\pi} \rfloor$, tel que $kn = a^2 + db^2$.

(c) Supposons tout d'abord que $p$ est un nombre premier impair de la forme $a^2+2b^2$. La question (a) implique alors que $-2$ est un carré modulo $p$, d'où $\left(\dfrac{-2}{p}\right) = 1$. Or

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$$

et d'après le cours, on a

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4 \\ -1 & \text{si } p \equiv 3 \pmod 4 \end{cases} \quad \text{et} \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod 8 \\ -1 & \text{si } p \equiv \pm 3 \pmod 4. \end{cases}$$

Donc finalement on obtient que

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv \pm 1 \pmod 8 \end{cases} \quad \text{ou} \quad \begin{cases} p \equiv 3 \pmod 4 \\ p \equiv \pm 3 \pmod 8 \end{cases}$$

On en déduit finalement que $p \equiv 1 \pmod 8$ ou $p \equiv 3 \pmod 8$.

Réciproquement, supposons que $p \equiv 1$ ou $3 \pmod 8$. Alors $-2$ est un carré modulo $p$ et la question (b) implique que l'un au moins des nombres

$$p, 2p, \ldots, hp$$

est de la forme $a^2+2b^2$, où $h = \lfloor \frac{4\sqrt{2}}{\pi} \rfloor$. Comme $1 \leq \frac{4\sqrt{2}}{\pi} < 2$, on a nécessairement $h = 1$. Autrement dit, $p$ est de la forme $a^2 + 2b^2$.

**Exercice 4**

(a) En appliquant la formule d'Abel à la fonction $f(t) = t^{-a}$, qui est de classe $C^1$ sur l'intervalle $[1, +\infty[$, et à la fonction arithmétique $a(n) = 1$, $n \geq 1$, on obtient

$$\sum_{n \leq x} \frac{1}{n^a} = A(x)f(x) - \int_1^x A(t)f'(t)\, dt.$$

Or $f'(t) = -at^{-a-1}$ et $A(x) = \sum_{n \leq x} a(n) = \lfloor x \rfloor$. D'où

$$\sum_{n \leq x} \frac{1}{n^a} = \frac{\lfloor x \rfloor}{x^a} + a \int_1^x \frac{\lfloor t \rfloor}{t^{a+1}}\, dt.$$

Introduisons maintenant la partie fractionnaire de $t$, $\{t\} = t - \lfloor t \rfloor$, ce qui donne

$$\begin{aligned}
\sum_{n \leq x} \frac{1}{n^a} &= x^{1-a} - \frac{\{x\}}{x^a} + a \int_1^x t^{-a}\, dt - a \int_1^x \frac{\{t\}}{t^{1+a}}\, dt \\
&= x^{1-a} - \frac{\{x\}}{x^a} + \frac{a}{1-a} x^{1-a} - \frac{a}{1-a} - a \int_1^x \frac{\{t\}}{t^{1+a}}\, dt \\
&= \frac{x^{1-a}}{1-a} - \frac{\{x\}}{x^a} - \frac{a}{1-a} - a \int_1^x \frac{\{t\}}{t^{1+a}}\, dt.
\end{aligned}$$

Remarquons que comme $1 + a > 1$, l'intégrale

$$\int_1^{+\infty} \frac{\{t\}}{t^{1+a}}\, dt$$

converge et si on note $L(a)$ sa limite, on a

$$\sum_{n \leq x} \frac{1}{n^a} = \frac{x^{1-a}}{1-a} - a\left(\frac{1}{1-a} + L(a)\right) - \frac{\{x\}}{x^a} + a \int_x^{+\infty} \frac{\{t\}}{t^{1+a}}\, dt.$$

Pour conclure, notons $\gamma(a) = a\left(\frac{1}{1-a} + L(a)\right) > 0$, et remarquons que

$$\int_x^{+\infty} \frac{\{t\}}{t^{1+a}}\, dt = O\left(\int_x^{+\infty} \frac{dt}{t^{1+a}}\right) = O(x^{-a}).$$

(b) Une intégration par partie donne

$$\int_2^x \frac{dt}{t^a \log t} = \frac{1}{1-a}\left[\frac{t^{1-a}}{\log t}\right]_2^x + \frac{1}{1-a} \int_2^x \frac{dt}{t^a (\log t)^2}.$$

La fonction $t \longmapsto \dfrac{1}{t^a(\log t)^2}$ étant décroissante, on a

$$\int_2^x \frac{dt}{t^a (\log t)^2} \leq \frac{1}{x^a (\log x)^2} x = \frac{x^{1-a}}{(\log x)^2}.$$

De plus, comme $1 - a > 0$, on a $\frac{2^{1-a}}{\log 2} = O\left(\frac{x^{1-a}}{(\log x)^2}\right)$. On obtient donc

$$\int_2^x \frac{dt}{t^a \log t} = \frac{x^{1-a}}{(1-a)\log x} + O\left(\frac{x^{1-a}}{(\log x)^2}\right).$$

(c) Appliquons cette fois ci la formule d'Abel avec la fonction arithmétique $a(n) = 1$ si $n = p$ est premier, 0 sinon. Alors $A(x) = \pi(x)$ et on a

$$\sum_{p \leq x} \frac{1}{p^a} = \frac{\pi(x)}{x^a} + a \int_2^x \frac{\pi(t)}{t^{1+a}}\, dt.$$

Par hypothèse, $R(t) := \pi(t) - \dfrac{t}{\log t} = O\left(\dfrac{t}{(\log t)^2}\right)$, d'où, en utilisant la question (b), on obtient

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p^a} &= \frac{x^{1-a}}{\log x} + \frac{R(x)}{x^a} + a \int_2^x \frac{dt}{t^a \log t} + a \int_2^x \frac{R(t)}{t^{1+a}}\, dt \\ &= \frac{x^{1-a}}{(1-a)\log x} + O\left(\frac{x^{1-a}}{(\log x)^2}\right) + a \int_2^x \frac{R(t)}{t^{1+a}}\, dt. \end{aligned}$$

Il reste à remarquer que

$$\int_2^x \frac{R(t)}{t^{1+a}}\, dt = O\left(\int_2^x \frac{dt}{t^a (\log t)^2}\right) = O\left(\frac{x^{1-a}}{(\log x)^2}\right).$$