Feuille d'exercices : *Arithmétique*

MPSI-Maths.
Mr Mamouni : *myismail1@menara.ma*

بِسمِ اللَّهِ الرَّحمَنِ الرَّحِيمِ
وَ قُلِ إِعمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُم وَ رَسوُلَهُ وَ المُؤ مِنِين

صَدَقَ اللَّهُ العَظِيم

Exercice 1. **Montrer les propriétés suivantes :**

1) $\forall (a,b,c) \in \mathbb{N}^3$ **:** (9 **divise** $a^3+b^3+c^3$) $\Rightarrow$ (3 **divise** a **ou** b **ou** c)
2) $\forall (a,b,c) \in \mathbb{N}^3$ **:** (**7 divise a** ^{3} **+ b** ^{3}**+ c** ^{3}) $\Rightarrow$ (**7divise** abc)
3) $\forall n \in \mathbb{N}$ **on a :** 6 **divise** $5n^3+n$
4) $\forall n \in \mathbb{N}$ **on a :** 9 **divise** $n^3+(n+1)^3+(n+2)^3$

Exercice 2. **Donner le chiffres des unités de** 4444^{4444}**.**
Indication : On pourra travailler dans $\mathbb{Z}/10\mathbb{Z}$.

On pose $N = 4444^{4444}$**.**
A **la somme des chiffres de** N, B **celle de** A **et** C **celle de** B**.**
Trouver C**.**
Indication : On pourra utiliser aprés l'avoir justifié qu'un nombre n ***et la somme de ses chiffres*** $\varphi(n)$ ***sont toujours congrus modulo*** 9***, et que si*** $n < 10^k$***, alors*** $\varphi(n) \leq 9k$

Exercice 3. **Soit** $N = 111111111$**, écrit en base** 10**.**
Justifier que : $N^2 = 12345678987654321$

Exercice 4. **.**

1) **Nous sommes le mercredi** $22-11-2007$**, l'année prochaine quel jour sera le** $22-10-2007$ **?**
2) **Dans quelle année le** $22-11$ **sera un mercredi ?**

Exercice 5. **Trouver tous les chiffres** x **et** y **qui vérifient :** $\overline{28x75y}^{10}$ **est divisible par 3 et par 11.**

Exercice 6. **Soit** $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$**, montrer que :**

$$a \wedge b = 1 \Leftrightarrow ab \wedge (a+b) = 1.$$

Exercice 7. **Résoudre dans** $\mathbb{N}^* \times \mathbb{N}^*$ **le systéme suivant :**

$$\begin{cases} x \geq y \\ x \vee y = (x \wedge y)^2 \\ x \vee y + x \wedge y = 156 \end{cases}$$

Exercice 8. **Soit** $n \in \mathbb{N}$**,on pose** $x = 3n+1, y = 5n-1$ **.**

1) **Montrer que** $x \wedge y$ **divise** 8.
2) **Trouver les entiers** n **tels que** $x \wedge y = 8$.

Exercice 9. **Soit** $n \in \mathbb{N}$**. Montrer que :**
2^n **divise** $\left(3+\sqrt{5}\right)^n + \left(3-\sqrt{5}\right)^n$**.**

Exercice 10. Soient $a, b \in \mathbb{N}^*$ premiers entre eux tels que ab est un carré parfait. Montrer que a et b sont des carrés parfaits.

Exercice 11. Soient $a, b \in \mathbb{N}^*$ et m, n premiers entre eux tels que $a^n = b^m$. Montrer qu'il existe $c \in \mathbb{N}^*$ tel que $a = c^m$ et $b = c^n$.

Exercice 12. Soient $a \in \mathbb{N}, a \geq 2, (m, n) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $m \geq n$. On pose $m = qn + r$ avec $0 \leq r < n$.

1) Montrer que : $\exists b \in \mathbb{N}$; $a^m - 1 = (a^n - 1)b + a^r - 1$.
2) Montrer que : $(a^m - 1) \wedge (a^n - 1) = a^{m \wedge n} - 1$.
3) Montrer que : $(a^n - 1)$ divise $(a^m - 1) \iff n$ divise m
4) Soit N_k le nombre qui s'écrit en base 10 avec k chiffres tous ègaux à 1.
   Montrer que : N_h divise $N_k \iff h$ divise k.

Exercice 13. Nombres de Fermat. ***mathématicien français, 1601-1665 :***

Les nombres de Fermat sont ceux de la forme : $F_n = 2^{2^n} + 1$

1) Montrer que tous ces nombres sont premiers entre eux deux à deux
2) Montrer que F_n est premier pour $n \in [|0, 4|]$ mais F_5 ne l'est pas
3) Soit $a \in \mathbb{N}^*$ montrer que si $2^a + 1$ est premier alors a est une puissance de 2

A l'heure actuelle on ne connait aucun nombre de Fermat premier autre que ceux de (2) mais on connait plusieurs qui ne le sont pas : F_{1945} qui a plus de 10582 chiffres est divisible par $2^{1947}5 + 1$qui a exactement 587 chiffres.

Exercice 14. Décomposition à coéfficients positifs :

Soient $a, b \in \mathbb{N}^*$ premiers entre eux.
Montrer que : $\forall\ x \geq ab$, $\exists\ u, v \in \mathbb{N}$ tels que $au + bv = x$.

Exercice 15. Crible d'Erathosténe

1) Montrer que tout entier supérieur à 2 non premier admet au moins un diviseur premier inférieur à sa racine.
2) Enoncer le ***crible d'Erathosténe*** qui permet de tester si un nombre est premier.
3) Donner les 20 premiers nombres premiers
4) Les nombres suivants sont - ils premiers : 353 , 91451

Exercice 16. Critère d'Eseinstein

1) Soient $(p, q) \in \mathbb{Z} \times \mathbb{N}$ tel que $p \wedge q = 1$ et $(ai)_{0 \leq i \leq n} \in \mathbb{N}^{n+1}$. Montrer que si $\frac{p}{q} \in \mathbb{Q}$ est solution de l'équation :

$$a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 = 0$$

   alors : p divise a_0 et q divise a_n
2) Résoudre l'équation : $30X^3 - 37X^2 + 15X - 2 = 0$

Exercice 17. Nombres de Mersenne :

Ils sont de la forme : $M_p = 2^p - 1$ avec p premier.

1) Montrer que les ***Nombres de Mersenne*** sont premiers entre eux deux à deux.
2) Soit $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que : $a^b - 1$ est premier, montrer alors que : $a = 2$ et b premier.

Le 11 Septembre 2006 fût découvert le plus grand nombre premier connu jusqu'à nos jours, c'est le nombre de Mersenne $M_{232\,582\,657} = 2^{232\,582\,657} - 1 = 124575026015369455 40 \ldots 11752880154053967871$, ***formé par*** 9 808 358, ***c'est le 44 ème nombre de Mersenne premier découvert, la méthode utilisé s'appelle GIMPS (Great Internet Mersenne Prime Search), qui consiste à utiliser plusieurs serveurs distants connectés via internet.***

Exercice 18. Théorème de Wilson.
Soit p un entier premier.

1) Montrer que $\forall\, \overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*, \quad \exists \overline{b} \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $\overline{a}\overline{b} = \overline{1}$.
2) En déduire que : $(p-1)! \equiv -1 (mod\ p)$.

Exercice 19. Cryptographie-RSA
Soit p et q deux nombres premiers, on pose $n = pq$. Soit M un entier naturel premier avec pq, qui représente le message à décoder, et C le message codé envoyé.

1) Dites pourquoi $\varphi(n) = (p-1)(q-1)$.
2) Soit e premier avec $\varphi(n)$, justifier l'existence de $d \in \mathbb{Z}$ tel que $ed \equiv 1 \pmod{\varphi(n)}$.
3) Le message M est codé en C tel que $C \equiv M^e \pmod{n}$. En déduire que : $C^d \equiv M \pmod{n}$.

Indication : On pourra penser à utiliser le théorème d'Euler.
Remarque : Le couple (n, e) est appelé clef publique alors que le couple (n, d) est appelé clef privée. On constate que pour chiffrer un message, il suffit de connaitre e et n. En revanche pour déchiffrer, il faut d et n. Ainsi il suffit de connaitre p, q et e puisque $\varphi(n) = (p-1)(q-1)$ et $d \equiv e^{-1} \quad [\varphi(n)]$.

Exercice 20. Petit Théorème de Fermat.
Soit p un nombre premier.

1) Montrer que p divise $\begin{pmatrix} p \\ k \end{pmatrix}$, $\quad \forall k \in [|1, p-1|]$.
   Indication : Utiliser le théorème de Gauss.
2) Montrer que pour tous $n, m \in \mathbb{N}^2$ on a : $(n+m)^p \equiv n^p + m^p \quad (mod\ p)$
3) Que peut-on dire alors de l'application $\phi : \begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \overline{x} & \longmapsto & \overline{x}^p \end{array}$.
4) Montrer que : $\forall n \in \mathbb{N} : n^p \equiv n \quad (mod\ p)$.

Exercice 21. Problème de Bezout :
Soient a, b, c trois entiers relatifs. On considère l'équation : $ax + by = c$, appelée problème de Bezout dont on recherche les solutions dans $\mathbb{Z}^2$.

1) Donner une condition nécéssaire et suffisante pour que cette équation admette une solution.
2) Soit (x_0, y_0) une solution particulière du problème de Bézout. Déterminer la forme générale des autres solutions (x, y) en fonction de $a, b, d = a \wedge b, x_0$ et y_0.
3) Résoudre dans $\mathbb{Z}^2$:
   a) $95x + 71y = 46$.
   b) $20x - 53y = 3$.
   c) $12x + 15y + 20z = 7$.
   d) $2520x - 3960y = 6480$.

Exercice 22. Congruences simultanées, théorème des restes chinois
Soient $a, b, n, m \in \mathbb{Z}$ avec $n \wedge m = 1$.
On considère le système : $\begin{cases} x \equiv a & (mod\ n) \\ x \equiv b & (mod\ m) \end{cases} \quad (S)$

1) Justifier l'existence de $(u, v) \in \mathbb{N}^2$, tel que $\begin{cases} nu \equiv 1 & (mod\ m) \\ mv \equiv 1 & (mod\ n) \end{cases}$.
2) En déduire que $x_0 = amv + bnu$ est une solution particulière du sytème ***(S)***.
3) Montrer que toutes les autres solutions sont congrues avec x_0 modulo nm.
4) Résoudre : $\begin{cases} x \equiv 2 & (mod\ 140) \\ x \equiv -3 & (mod\ 99) \end{cases}$

Exercice 23. Théorème des restes chinois généralisé :

Soient $m_1, \dots, m_n$ des entiers deux à deux premiers entre eux, on se propose de résoudre le système suivant d'inconnue $x \in \mathbb{Z}$:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \quad (S)$$

1) **Montrer que :** $\forall i \in [|1,n|], \exists u_i \in \mathbb{N}$ **tel que** $M_i u_i \equiv 1 \pmod{m_i}$, **où** $M_i = \dfrac{M}{m_i}$, **avec** $M = \prod_{i=1}^{n} m_i$.

2) **Montrer que** $x_0 = \sum_{i=1}^{n} a_i M_i u_i$ **est solution particulière de** $(\mathcal{S})$.

3) **Montrer que toutes les autres solutions de** $(\mathcal{S})$ **sont congrues à** $x_0 \mod M$, **en déduire l'ensemble de solutions du sytéme.**

4) ***Origine de l'appelation.***
Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces.
Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces.
Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces.
Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?
Réponse : 785

Exercice 24. p-valuation.

Soient $n \geq 2$ et p premier, on appelle p-valuation de n, l'entier $v_p(n)$ égale à la puissance de maximale de p qui divise n.
Exemple : $v_2(8) = 3, v_2(12) = 2$.

1) **Que vaut** $v_p(n)$ **si** $n \wedge p = 1$
2) **Justifier que** $\forall i \in \mathbb{N}, \quad p^i$ **divise** $n \Longrightarrow i \leq v_p(n)$.
3) **Montrer que pour tout** $x \in \mathbb{R}$ **et** $n \in \mathbb{N}^*$, **on a :**

$$E\left(\frac{E(nx)}{n}\right) = E(x)$$

4) **En déduire que** $\forall (i,j) \in \mathbb{N}^2$ **:**

$$p^{i+j} \leq n \Longrightarrow E\left(\frac{1}{p^j} E\left(\frac{n}{p^i}\right)\right) = E\left(\frac{n}{p^{i+j}}\right)$$

5) **On pose** $m = E\left(\frac{n}{p}\right)$, **montrer que :** $v_p(n!) = m + v_p(m!)$.
6) ***Applications :***
   a) **Calculer** $v_7(10000!)$
   b) **Décomposer** $16!$ **en produits de facteurs premiers.**
   c) **Montrer qu'en base** 10, $1000!$ **se termine par** 249 **zéros.**

Exercice 25. Produit de Dirichlet et Formule d'inversion de Moebius.

- Une fonction $f : \mathbb{N}^* \longrightarrow \mathbb{N}$ est dite arithmétique multiplicative ***si et seulement si*** elle vérifie la relation suivante : $f(nm) = f(n)f(m)$, pour tous n, m tel que $n \wedge m = 1$.
- On notera par $\mathcal{M}$, l'ensemble de telles fonctions, surlequel on définit l'opération suivante $(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$ appelée Produit de Dirichlet.
- Pour tout $n \in \mathbb{N}^*$ on note par $\mathcal{D}_n$ l'ensemble de ses diviseurs dans $\mathbb{N}$
- La fonction de Moebius est définit pour tout $n \in \mathbb{N}^*$ par la relation suivante :
  $\mu(n) = 0$ si $\exists p$ premier tel que p^2 divise n
  $= (-1)^r$sinon, où r désigne le nombre des diviseurs premiers de n

1) Montrer que $*$ définit sur $\mathcal{M}$ une LCI, puis une structure de groupe abélien d'élément neutre l'application $e(n) = 0$ si $n \neq 1$ et $e(1) = 1$.
2) Montrer que $*$ est distributive par rapport à $+$.
3) Montrer que $\mu * 1 = e$ où 1 est la fonction constante sur $\mathbb{N}^*$ égale à 1.
4) Soient $f, g \in \mathcal{M}$ tel que $g(n) = \sum_{d|n} f(d)$ pour tout $n \in \mathbb{N}^*$, montrer alors que :

$$f(n) = \sum_{d|n} \mu(d)g\left(\frac{d}{n}\right) \quad \text{Formule d'inversion de Moebius}$$

Exercice 26. Fonction indicatrice d'Euler.

l'indicateur d'Euler d'un entier positif n, noté $\varphi(n)$ est défini comme étant le nombre d'entiers positifs inférieurs ou égaux à n et premiers avec n.

1) Montrer que p premier ***si et seulement si*** $\varphi(p) = p - 1$.
2) Soit p premier et $\alpha \in \mathbb{N}$. Donner tous les multiples de p inférieurs à p^α, puis en déduire que : $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.
3) Soit $f : \begin{array}{ccc} [|1,n|] & \longrightarrow & \mathcal{D}_n \\ k & \longmapsto & k \wedge n \end{array}$, où $\mathcal{D}_n$ est l'ensemble des diviseurs de n dans $\mathbb{N}$.
   Montrer que tout élèment de $\mathcal{D}_n$ admet exactement $\varphi\left(\frac{n}{d}\right)$ antécédants par f.
4) En déduire que $n = \sum_{d|n} \varphi(d)$, pour tout $n \in \mathbb{N}^*$.
5) En déduire que $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$, pour tout $n \in \mathbb{N}^*$.
6) Soit $(m, n) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $n \wedge m = 1$.
   Montrer que $\varphi(nm) = \varphi(n)\varphi(m)$.
7) Soient $p_1, \ldots, p_r$ des nombres premiers, $\alpha_1, \ldots, \alpha_r$ des entiers naturels et, $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.
   En déduire $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.
8) Soit $a \in \mathbb{N}^*$ premier avec n, montrer que :

$$a^{\varphi(n)} \equiv 1 \pmod{n} \qquad \text{Théorème d'Euler.}$$

Exercice 27. Fonctions arithmétiques multiplicatives.

- **Une fonction** $f : \mathbb{N}^* \longrightarrow \mathbb{N}$ **est dite arithmétique multiplicative** ***si et seulement si*** **elle vérifie la relation suivante :** $f(nm) = f(n)f(m)$**, pour tous** n, m **tel que** $n \wedge m = 1$**.**
- **Pour tout** $n \in \mathbb{N}^*$ **on note par** $\mathcal{D}_n$ **l'ensemble de ses diviseurs dans** $\mathbb{N}$
- **Soit** $n \in \mathbb{N}^*$**, on note par** $\phi(n)$ **la somme des diviseurs de** n **dans** $\mathbb{N}$
  $\phi(n) = \sum_{d|n} d$**.**

1) **Montrer que** n **est premier** ***si et seulement si*** $\phi(n) = n+1$**.**
2) **Soit** $a, b, c \in \mathbb{N}^*$ **tel que** $a \wedge b = 1$**.**
   Montrer que : $a \wedge (bc) = a \wedge c$ **.**
   $(ab) \wedge c = (a \wedge c)(b \wedge c)$
3) **Soit** $(m, n) \in \mathbb{N}^* \times \mathbb{N}^*$ **tel que** $n \wedge m = 1$**.**
   a) **Montrer que les applications**
   $$\begin{array}{rccc} \psi_1 : & \mathcal{D}_n \times \mathcal{D}_m & \longrightarrow & \mathcal{D}_{nm} \\ & (p, q) & \longmapsto & pq \end{array}$$
   $$\begin{array}{rccc} \psi_2 : & \mathcal{D}_{nm} & \longrightarrow & \mathcal{D}_n \times \mathcal{D}_m \\ & d & \longmapsto & (d \wedge n, d \wedge m) \end{array}$$
   sont isomorphes l'une de l'autre.
   b) **En déduire que**
   card$(D(nm))$ = **card**$(D(n))$**card**$(D(m))$**.**
   c) **Tout diviseur** d **de** nm **s'écrit sous la forme** $d_1 d_2$ **où** d_1 **divise** n **et** d_2 **divise** m**.**
   d) **En deduire que l'application :**
   $$\begin{array}{rccc} f : & D(n) \times D(m) & \longrightarrow & D(nm) \\ & (d_1, d_2) & \longmapsto & d_1 d_2 \end{array}$$
   est bijective.
   e) **En deduire aussi que :** $\phi(nm) = \phi(n)\phi(m)$
4) **Soit** p **premier et** $\alpha \in \mathbb{N}$**, Donner tous les diviseurs de** p^α**, puis en déduire** $\phi(p^\alpha)$**.**
5) **Soient** $p_1, \ldots, p_r$ **des nombres premiers et** $\alpha_1, \ldots, \alpha_r$ **des entiers naturels, en déduire** $\phi(n)$ **où** $n = \prod_{i=1}^{r} p_i^{\alpha_i}$**.**

Exercice 28. Nombres d'Euclide et nombres parfaits.

- **Pour tout** $n \in \mathbb{N}^*$ **on note par** $\mathcal{D}_n$ **l'ensemble de ses diviseurs dans** $\mathbb{N}$
- **Soit** $n \in \mathbb{N}^*$**, on note par** $\phi(n)$ **la somme des diviseurs de** n **dans** $\mathbb{N}$
  $\phi(n) = \sum_{d|n} d$
- **Soit** $n \in \mathbb{N}^*$**. On dit que** ***n*** **est parfait** ***ssi*** $\phi(n) = 2n$ **.**
- **On appelle** ***Nombre d'Euclide*** **tout entier naturel de la forme** $2^{p-1}(2^p - 1)$ **tel que** p **et** $2^p - 1$ **soient premiers.**

1) **Soit** $E_p = 2^{p-1}(2^p - 1)$ **un** ***nombre d'Euclide.***
   Trouver tous les diviseurs de E_p **.**
2) **En déduire que les** ***nombres d'Euclide*** **sont tous parfaits**
3) **Soit** ***N*** **un nombre parfait pair.**
   a) **Montrer que :** $\exists m \in \mathbb{N}, \quad \exists q \quad impair$ **tel que :** $N = 2^m q$
   b) **Montrer que** $\exists r \in \mathbb{N}^*$ **tel que** $q = (2^{m+1} - 1)r$ **et** $\phi(q) = 2^{m+1} r$**.**
   On pourra utiliser le fait que ***N*** **est parfait.**
   c) **Montrer que** ***r=1.***
   d) **Montrer que** $p, 2^p - 1$ **sont premiser où** ***p=m+1***
   e) **Conclure. A l'heure actuelle on ne sait pas s'ils existent des nombres parfaits impairs**

Fin.