FICHE 1

Rappels et compléments d'arithmétique

Dans les exercices suivants, $O_n(x)$ *représente l'ordre de* x *dans le groupe* $(\mathbb{Z}/n\mathbb{Z})^\times$ *des éléments inversibles de* $\mathbb{Z}/n\mathbb{Z}$*, défini pourvu que* x *soit premier avec* n*. On dit que* g *est un* générateur *de* $\mathbb{Z}/n\mathbb{Z}$ *si* $(\mathbb{Z}/n\mathbb{Z})^\times$ *est cyclique engendré par* g*.*

Exercice 1.1 Démontrer la propriété d'associativité suivante de la la division euclidienne :

$$(a : b) : c = a : (bc).$$

Exercice 1.2 Calculer l'inverse de 13 modulo 100.

Exercice 1.3 Résoudre les équations

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

Exercice 1.4 Résoudre $42x + 150y = 18$.

Exercice 1.5

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

Exercice 1.6 Simplifier l'expression $\mathrm{pgcd}(11\,a + 5\,b, 13\,a + 6\,b)$.

Exercice 1.7 Le produit de trois entiers consécutifs peut–il être un carré ?

Exercice 1.8 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 1.9 Démontrer le théorème de Wilson :

Pour que p soit premier, il faut et il suffit que $(p-1)! \equiv -1 \pmod p$.

Exercice 1.10 Soit $p \geq 3$ premier. Montrer que le numérateur de la fraction irréductible égale à

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

est divisible par p. On peut démontrer, plus difficilement, que ce numérateur est en fait divisible par p^2.

Exercice 1.11 Soit a, b, c, d des entiers naturels tels que $\frac{a}{b} < \frac{p}{q} < \frac{c}{d}$, et $bc - ad = 1$.

1. Démontrer que $q > \max(b, d)$.
2. Démontrer que la fraction de plus petit dénominateur, comprise strictement entre $\frac{a}{b}$ et $\frac{c}{d}$, est la fraction $\frac{a+c}{b+d}$.

Application :

1. Donner un algorithme pour trouver la fraction de plus petit dénominateur appartenant à $]u, v[$, avec u, v réels et $u < v$.
2. Quelle est la fraction dont le dénominateur ne dépasse pas 10, qui est la plus proche de 6.55957 ?

Exercice 1.12 Démontrer que $H_n = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ n'est jamais un entier.
Soit $V = \mathrm{ppcm}(1, 2, \ldots, n)$. On écrit

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \frac{U}{V}$$

avec U entier. Soit 2^a la plus grande puissance de 2 inférieure ou égale à n.

1. Démontrer que pour tout entier k, $1 \leq k \leq n$, on a $\mathrm{v}_2(k) \leq a$, avec égalité si et seulement si $k = 2^a$.
2. Quelle est la valeur de $\mathrm{v}_2(V)$?
3. Soit k un entier $1 \leq k \leq n$, et U_k l'unique entier tel que $\frac{1}{k} = \frac{U_k}{V}$. Exprimer la valeur de $\mathrm{v}_2(U_k)$ au moyen de $\mathrm{v}_2(k)$.
4. En déduire que U est un nombre impair et que H_n n'est pas un entier.

Exercice 1.13 Soit $x \in \mathbb{R}$ et des entiers $a_1, a_2, \dots, a_n$ tous $\leq x$ et tels que aucun des a_1, $1 \leq i \leq n$ ne divise le produit des autres. Démontrer que $n \leq \pi(x)$, où $\pi(x)$ est le cardinal de l'ensemble des nombres premiers $\leq x$.

Exercice 1.14 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 1.15 Expliciter un n tel que $n, n+1, n+2, \dots, n+9$ soient tous non premiers :

1. En supposant d'abord que vous ignorez le théorème des restes chinois.
2. En utilisant le théorème des restes chinois.

Exercice 1.16 a et b sont premiers entre eux et $\in \mathbb{N}$. On considère l'équation

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

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

Exercice 1.18

1. 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 $x^2 \equiv x \pmod{10000}$?
2. Si vous ne l'avez pas remarqué, vérifiez que x est solution de $x^2 - x \equiv 0 \pmod{N}$ si et seulement si $1 - x$ est solution. Retrouvez ainsi sans calcul le résultat précédent.

Exercice 1.19 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 1.20 Résoudre le système de congruences

$$\begin{cases} x & \equiv & a & \pmod{3} \\ x & \equiv & b & \pmod{5} \\ x & \equiv & c & \pmod{7} \end{cases}$$

Exercice 1.21 Résoudre le système de congruences avec un minimum de calculs :

$$\begin{cases} 5x & \equiv & 6 & \text{mod} & 7 \\ 7x & \equiv & 8 & \text{mod} & 9 \\ 9x & \equiv & 10 & \text{mod} & 11 \\ 11x & \equiv & 12 & \text{mod} & 13 \end{cases}$$

Exercice 1.22 Démontrer que si vous disposez d'un algorithme de calcul efficace de $\varphi(n)$, alors vous pouvez rapidement factoriser les entiers qui sont le produits de deux facteurs premiers.

Exercice 1.23 (Tiré de la rubrique de jeux mathématiques du *Monde*)

1. Vérifier qu'il n'existe qu'un multiple de 4, plus petit 100 dont l'écriture décimale n'utilise que les chiffres 1 et 2
2. Déterminer tous les multiples de 8, plus petits que 1000, dont l'écriture décimale n'utilise que les chiffres 1 et 2.
3. Démontrer que pour tout entier $n \geq 1$ il n'existe un unique multiple de 2^n dont l'écriture décimale utilise exactement n chiffres appartenant tous à $\{1, 2\}$.

Exercice 1.24

1. Soit n un entier naturel dont l'écriture en base 10 est $n = \overline{c_k c_{k-1} \dots c_1 c_0}$. Montrer que le nombre $c_k + c_{k-1} + \dots + c_1 + c_0$ est congru à n modulo 9.
2. Soit n un entier naturel dont l'écriture en base 10 est $n = \overline{c_k c_{k-1} \dots c_1 c_0}$. Montrer que le nombre $c_0 - c_1 + c_2 - \dots + (-1)^k c_k$ est congru à n modulo 11.

Exercice 1.25 Soit $A = 4444^{4444}$. Soit B la somme des chiffres de A, C la somme des chiffres de B et enfin D la somme des chiffres de C. Calculer D.

Exercice 1.26 Comment calculer rapidement les 40 premiers facteurs premiers de $10^{10^9} - 1$.

Exercice 1.27 Soit m un entier impair non multiple de 5.

1. Montrer qu'il existe un multiple entier de m dont l'écriture décimale ne comporte que des 9.
2. Montrer qu'il existe un multiple entier de m dont l'écriture décimale ne comporte que des 1.

Exercice 1.28 Trouver les deux derniers chiffres de $39^{39^{39}}$. Même question avec $17^{17^{17}}$.

Exercice 1.29 Montrer que si n est impair alors $n \mid 2^{n!} - 1$.

Exercice 1.30 Soit n un entier positif ou nul.

1. Démontrer la formule de Legendre :

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

2. Prouver que chacun des termes de la suite $\left(\left\lfloor \frac{n}{p^k} \right\rfloor \right)$ est le quotient de la division euclidienne du précédent par p.
3. Ecrire en `Sage` la fonction `vpfact(n,p)` qui renvoie la valuation en p de $n!$.

Exercice 1.31 1. Par combien de zéros se termine 2002! ?

2. $\binom{1000}{500}$ est-il divisible par 7 ?
3. Déterminer $\mathrm{v}_2((2^n - 1)!)$ c'est à dire l'exposant de 2 dans la décomposition en facteurs premiers de $(2^n - 1)!$.
4. Montrer que $4 \,\Big|\, \binom{2n}{n}$ si n n'est pas une puissance de 2.

Exercice 1.32 Montrer que si p est premier impair, le produit de deux générateurs de $(\mathbb{Z}/p\mathbb{Z})^\times$ n'est pas un générateur.

Exercice 1.33 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 $\mathbb{F}_q$ (indication : considérer l'ordre de a dans $\mathbb{F}_q$).

Exercice 1.34 Montrer que si p est un nombre premier impair alors, pour tout k :

$$O_p(2^k) = O_p\left(\left(\frac{p+1}{2} \right)^k \right)$$

Exercice 1.35 Expliciter un générateur multiplicatif de $\mathbb{Z}/4913\mathbb{Z} = \mathbb{Z}/17^3\mathbb{Z}$.

Exercice 1.36 Montrer que si p est premier, $(a, p) = 1$, et $4 \mid O_p(a)$ 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 générareur.

Exercice 1.37 Montrer qu'il n'existe pas d'entier $n > 1$ tel que $n \mid (2^n - 1)$. Indication : considérer le plus petit diviseur premier de n.

Exercice 1.38 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.

Exercice 1.39 Montrer que toute progression arithmétique infinie d'entiers positifs contient k termes consécutifs tous composés. Vous pourrez utiliser le théorème des restes chinois, en remarquant qu'une condition suffisante pour que $a + bx$ soit non premier est que $a + bx \equiv 0 \pmod p$, avec p premier (pourvu que $p \neq a + bx$).

Exercice 1.40 Montrer que si $x \equiv p \pmod{p^2}$ avec p premier, alors x n'est pas de la forme y^n, $n \geq 2$. En déduire que pour tout k, il existe k entiers consécutifs qui ne sont pas des puissances. Indication : On pourra résoudre le système $x + i \equiv p_i \bmod p_i^2$, $i = 1, \ldots, k$

Exercice 1.41 Soit $n \geq 2$ un entier et $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $p_1 < p_2 < \ldots < p_k$ sa décomposition en produit de facteurs premiers. On rappelle l'expression de la fonction d'Euler, $\varphi(n)$ qui compte les entiers $\leq n$ et premiers avec n :

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{\alpha_i - 1}.$$

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

Exercice 1.42 (Nombre de retenues dans une addition) Soit p entier, $p \geq 2$. On s'intéresse à l'addition des entiers en base p. Soit A, B deux entiers de la forme

$$A = \sum_{k=0}^{r} a_k p^k \quad \text{et} \quad B = \sum_{k=0}^{r} b_k p^k.$$

Les écritures en base p de A et B sont donc respectivement

$$a_r \ldots a_1 a_0 \quad \text{et} \quad b_r \ldots b_1 b_0.$$

On note $A_1 = \sum_{k=1}^{r} a_k p^k$ (resp. $B_1 = \sum_{k=1}^{r} b_k p^k$) le quotient de la division euclidienne de A par p (resp. de B par p). Les écritures en base p de A_1 et B_1 sont donc

$$a_r \ldots a_1 \quad \text{et} \quad b_r \ldots b_1$$

Pour tout couple d'entiers naturels U, V on note $\mathrm{r}(U, V)$ le nombre de retenues dans l'addition en base p de U et de V. Démontrez que

1. Si $a_0 + b_0 < p$ on a $\mathrm{r}(A, B) = \mathrm{r}(A_1, B_1)$
2. Si $a_0 + b_0 \geq p$, soit $\alpha \geq 0$ la valuation en p de $A_1 + B_1 + 1$ c'est à dire le plus grand entier α tel que p^α divise $A_1 + B_1 + 1$. Démontrer que
$$\mathrm{r}(A, B) = 1 + \alpha + \mathrm{r}(A_1, B_1)$$

Exercice 1.43 (Un autre théorème de Lucas) Soit p un nombre premier fixé. Pour tout entier $n \geq 1$ on notera $\mathrm{V}(n)$ la valuation en p de $n!$ c'est à dire

$$\mathrm{V}(n) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots$$

Soient $m, n, a, b \in \mathbb{N}$ avec a et b strictement inférieurs à p. Montrer que

1. Pour $A_1 \in \mathbb{N}$ et $a_0 \in \{0, 1, \dots, p-1\}$ prouver que $\mathrm{V}(A_1 p + a_0) = A_1 + \mathrm{V}(A_1)$
2. Soient A_1, B_1 dans $\mathbb{N}$ et a_0, b_0 dans $\{0, 1, \dots, p-1\}$. Prouver que
$$\mathrm{V}[(A_1 p + a_0) + (B_1 p + b_0)] = \begin{cases} A_1 + B_1 + \mathrm{V}(A_1 + B_1) & \text{si } a_0 + b_0 < p \\ A_1 + B_1 + 1 + \mathrm{V}(A_1 + B_1 + 1) & \text{si } a_0 + b_0 \geq p \end{cases}$$
3. En déduire que
$$\mathrm{V}\Big((A_1 p + a_0) + (B_1 p + b_0)\Big) - \mathrm{V}(A_1 p + b_0) - \mathrm{V}(B_1 p + b_0) =$$
$$\begin{array}{rrll} & \mathrm{V}(A_1 + B_1) & -\mathrm{V}(A_1) - \mathrm{V}(B_1) & \text{si} \quad a_0 + b_0 < p \\ 1 & +\mathrm{V}(A_1 + B_1 + 1) & -\mathrm{V}(A_1) - \mathrm{V}(B_1) & \text{si} \quad a_0 + b_0 \geq p \end{array}$$
4. Notons $\mathrm{W}(A, B) = \mathrm{V}\left(\binom{A+B}{A}\right) = \mathrm{W}\left(\frac{(A+B)!}{A!\,B!}\right)$. En utilisant l'exercice 1.42, démontrer que $\mathrm{W}(A, B)$ est égal au nombre de retenues dans l'addition de A et B en base p.
5. En déduire que $\binom{n}{k}$ est premier avec p si et seulement si les chiffres de l'écriture en base p de n sont supérieurs ou égaux aux chiffres de l'écriture en base p de k.

Exercice 1.44 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 1.45 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 1.46 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 1.47 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 $(\mathbb{Z}/n\mathbb{Z})^\times$ est un diviseur de $n-1$.
2. Soit p un diviseur premier impair de n et $\alpha = \mathrm{v}_p(n)$ 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 $(\mathbb{Z}/n\mathbb{Z})^\times$ 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 $n-1$.