CHAPITRE 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 $\text{pgcd}(11\,a + 5\,b, 13\,a + 6\,b)$.

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

1. Démontrer le théorème de Wilson :
   Pour que p soit premier, il faut et il suffit que $(p-1)! \equiv -1 \pmod{p}$.
2. Soit $p \geq 3$ premier. Montrer que le numérateur de la fraction irréductible de valeur
$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$
est divisible par p.
On peut démontrer, plus difficilement, que ce numérateur est en fait divisible par p^2 (théorème de Wolstenholme).

Exercice 1.10 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 contenue dans un segment $]u, v[$, 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 ?
3. Soit $[u, v]$ un intervalle réel. Donner un algorithme rendant la fraction de plus petit dénominateur appartenant à cet intervalle.

Exercice 1.11 Démontrer que $H_n = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ n'est jamais un entier (réduire au même dénominateur toutes ces fractions, et étudier les parités du numérateur et du dénominateur).

Exercice 1.12 Soit $x \in \mathbb{R}$ et des entiers $a_1, a_2, \ldots, a_n$ 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 1.13 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 1.14 Prouver qu'il existe une infinité de premiers de la forme $4k - 1$. Exhiber une autre progression arithmétique $ak + b$ contenant une infinité de premiers.

Exercice 1.15 Expliciter un n tel que $n, n+1, n+2, \ldots, n+9$ 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

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

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

Exercice 1.18 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 $x^2 \equiv x \pmod{10000}$?

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 :

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

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 $c_k + c_{k-1} + \cdots + c_1 + c_0$ 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 $c_0 - c_1 + c_2 - \cdots + (-1)^k c_k$ 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 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 1.27 Trouver les deux derniers chiffres de $39^{39^{39}}$. Même question avec $17^{17^{17}}$.

Exercice 1.28 Montrer que si n est impair alors $n \mid 2^{n!} - 1$.

Exercice 1.29 1. Par combien de zéros se termine 2002! ?

2. $\binom{1000}{500}$ est-il divisible par 7 ?
3. Déterminer $v_2((2^n-1)!)$ c'est à dire l'exposant de 2 dans la décomposition en facteurs premiers de $(2^n-1)!$.
4. Montrer que $4 \mid \binom{2n}{n}$ si n n'est pas une puissance de 2.

Exercice 1.30 Montrer que

1. $11 \mid n^{11} + 10n$
2. $42 \mid n^7 - n$
3. $p \mid n^{p^p} - n$ (p est premier)
4. Montrer que si p et q sont premiers distincts, $pq \mid n^{pq} - n^p - n^q + n$.

Exercice 1.31 Montrer que si p est premier impair, le produit de deux générateurs de $\mathbb{Z}/p\mathbb{Z}$ n'est pas un générateur.

Exercice 1.32 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 1.33 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 1.34 Montrer que si p est un nombre premier impair, si $(a,p) = 1$ et si $O_p(a)$ est impair alors $a^x + 1 \equiv 0 \bmod p$ n'a pas de solution.

Exercice 1.35 Soit p un nombre premier et $d \geq 1$ un diviseur de $p-1$. Montrer que l'équation $x^d = 1$ a exactement d solutions dans $\mathbb{F}_p$.

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 génénrareur.

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 Soit p premier. Montrer que a est d'ordre 3 modulo p si et seulement si $a + 1$ est d'ordre 6.

Exercice 1.39 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 1.40 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 1.41 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 1.42 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 1.43 On appelle $n^{ième}$ 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. *Cette question suppose connu le chapitre du cours sur les carrés de $\mathbb{Z}/p\mathbb{Z}$:* En considérant le caractère quadratique de 2 modulo p montrer qu'on a un peu mieux : montrer que si p est un diviseur premier de F_n et $p = 1 + k2^{n+1}$ alors k est pair. Ainsi 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 1.44 (Un autre théorème de Lucas) 1. Soit p premier, $0 \leq a \leq p-1$ et $0 \leq b \leq p-1$. Montrer que pour tous n et k on a

$$\binom{np+a}{kp+b} \equiv \binom{n}{k}\binom{a}{b} \pmod{p}$$

avec la convention

$$\binom{a}{b} = 0 \text{ si } b > a.$$

Indication : considérer le coefficient de x^{kp+b} dans le développement de $(1+x)^{np+a}$, et utiliser l'identité (avec p premier)

$$(1+x)^p \equiv 1 + x^p \pmod{p}$$

2. Soient $A = \sum_{i=0}^{r} a_i p^i$ et $B = \sum_{i=0}^{r} b_i p^i$ les écritures en base p de A et B. Montrer que

$$\binom{A}{B} \equiv \prod_{i=0}^{r} \binom{a_i}{b_i} \pmod{p}$$

3. En déduire que p divise $\binom{A}{B}$ si et seulement si il existe un chiffre de l'écriture en base p de B qui est plus grand que le chiffre de même rang de l'écriture en base p de A.