Résumé de cours
Arithmétique
L2 (2004/2005)

Stéphane LOUBOUTIN
Bureau 112, I.M.L.
loubouti@iml.univ-mrs.fr

March 14, 2005

Contents

1 Polynômes, fractions rationnelles et séries formelles **5**
1.1 Structures 5
1.2 Polynômes 5
1.3 Fractions rationnelles 6
1.4 Séries formelles 8
1.5 Applications arithmétiques 8

2 Éléments d'arithmétique **11**
2.1 Vocabulaire 11
2.1.1 Nombres de Mersenne et de Fermat 12
2.1.2 Infinitude des nombres premiers 13
2.2 Le Théorème fondamental de l'arithmétique 14
2.2.1 Existence de la décomposition en facteurs premiers, mais unicité? 14
2.2.2 Existence et unicité de la décomposition en facteurs premiers 14
2.3 Le petit théorème de Fermat 17
2.4 Développements en base $b \geq 2$ 18
2.5 Calcul efficace de x^m modulo n pour m grand 18

3 Calculs modulaires et classes de congruences **21**
3.1 Le théorème chinois des restes 21
3.2 Définition des classes de congruence 22
3.3 Groupes, anneaux commutatifs unitaires et leurs groupes d'unités 23

4 Groupes abéliens finis **27**
4.1 Ordre d'un élément dans un groupe 27
4.2 Certificats de primalité 33
4.3 Cryptographie à clé révélée 35

5 Structure de $\mathbf{Z}_n^*$ **35**
5.1 Structure de $\mathbf{Z}_{p^n}^*$ 35
5.2 Structure de $\mathbf{Z}_{2^n}^*$ 36
5.3 Structure de $\mathbf{Z}_n^*$ 36

6 Nombres de Carmichael **37**

7 Tests de primalité probabilistes **39**

8 Sujets d'examen **41**

1 Polynômes, fractions rationnelles et séries formelles

1.1 Structures

Définition des structures d'anneau (commutatif ($ab = ba$), unitaire (il existe $1_{\mathbf{A}} \in \mathbf{A}$ tel que $1_{\mathbf{A}} \cdot a = a \cdot 1_{\mathbf{A}} = a$ pour tout $a \in \mathbf{A}$), intègre ($ab = 0$ implique $a = 0$ ou $b = 0$), éléments inversibles (il existe $b \in \mathbf{A}$ tel que $ab = ba = 1_{\mathbf{A}}$), $\cdots$) et de corps. Groupe multiplicatif $(\mathbf{A}^*, \cdot)$ des unités (=des inversibles) d'un anneau unitaire $\mathbf{A}$. Exemple, fondamental pour ce semestre, d'anneaux : les $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$, $n \geq 1$ entier. Ce sont les ensembles de symboles $\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ munis des opérations $+$ et $\cdot$ définies par $\overline{a}+\overline{b} = \overline{r}$ et $\overline{a}\cdot\overline{b} = \overline{r'}$ où r et r' désignent respectivement les restes des divisions euclidiennes de $a + b$ et ab par n. Ce sont des anneaux commutatifs unitaires (de neutres $\overline{0}$ pour $+$ et $\overline{1}$ pour $\cdot$) finis contenant n éléments. Ils ne sont en général pas intègres et pas des corps :

Exercice 1 *Montrer qu'un corps est un anneau intègre. Montrer que si $n = n_1 n_2 > 1$ n'est pas premier (avec $n_1 > 1$ et $n_2 > 1$), alors l'anneau $(\mathbf{Z}_n, +, \cdot)$ n'est pas intègre et n'est pas un corps. Donner les listes des inversibles des deux anneaux $(\mathbf{Z}_4, +, \cdot)$ et $(\mathbf{Z}_5, +, \cdot)$ (dresser d'abord les tables de multiplication dans ces anneaux). Lequel des deux est un corps?*

1.2 Polynômes

Soit $(\mathbf{A}, +, \cdot)$ un **anneau commutatif** et **unitaire**. On note $\mathbf{A}[X]$ l'ensemble des polynômes à coefficients dans $\mathbf{A}$, c'est à dire l'ensemble des expressions de la forme $P(X) = a_n X^n + \cdots + a_1 X + a_0 = \sum_{k=0}^{n} a_k X^k$, avec les a_i dans $\mathbf{A}$. Le **degré** de $P(X) \neq 0$ est alors le plus grand indice k pour lequel $a_k \neq 0$. Sur $\mathbf{A}[X]$ on définit $+$ et $\cdot$ qui munissent $\mathbf{A}[X]$ d'une structure d'anneau commutatif en posant $(a_n X^n + \cdots + a_1 X + a_0) + (a'_n X^n + \cdots + a'_1 X + a'_0) = (a_n + a'_n) X^n + \cdots + (a_1 + a'_1) X + (a_0 + a'_0)$ et $(a_m X^m + \cdots + a_1 X + a_0) \cdot (b_n X^n + \cdots + b_1 X + b_0) = c_{m+n} X^{m+n} + \cdots + c_1 X + c_0$ avec

$$c_k = \sum_{\substack{i+j=k \text{ et} \\ 0 \leq i \leq m,\ 0 \leq j \leq n}} a_i b_j.$$

Exercice 2 *Rappelons la formule du binôme*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k,$$

valable dans tout anneau unitaire commutatif. Dans ce qui suit, on choisit $a = 1$ et $x \in \mathbf{R}$.

1. *Montrer que $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.*
2. *En remarquant que $(1+x)^{2n} = (1+x)^n (1+x)^n$, montrer que $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.*
3. *Montrer en dérivant $(1+x)^n$ que $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$. Montrer de même que $\sum_{k=0}^{n} k^2 \binom{n}{k} = n(n+1)2^{n-2}$.*
4. *Montrer que $\sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k} = \frac{2^{n+1}-1}{n+1}$.*

Division euclidienne, par un polynôme $Q(X) = a_n X^n + \cdots + a_0$ avec $a_n \in \mathbf{A}^*$, dans $\mathbf{A}$ anneau commutatif unitaire, polynômes irréductibles, critère d'Eisenstein d'irréductibilité dans $\mathbf{Z}[X]$, décomposition en produit d'irréductibles dans $\mathbf{K}[X]$.

Une **racine** de $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbf{A}[X]$ dans $\mathbf{A}$ est un $\alpha \in \mathbf{A}$ tel que $P(\alpha) = 0$, qui implique $P(X) = P(X) - P(\alpha) = \sum_{k=0}^{n} a_k (X^k - \alpha^k) = (X - \alpha) Q(X)$ avec $Q(X) = \sum_{k=1}^{n} a_k \sum_{l=0}^{k-1} \alpha^l X^{k-1-l} \in \mathbf{A}[X]$, et réciproquement. Maintenant, si $\beta \in \mathbf{A}$ alors $P(\beta) = 0$ si et seulement si $(\alpha - \beta) Q(\beta) = 0$. Si $\mathbf{A}$ est un anneau **intègre** (c'est à dire que si $ab = 0$ dans $\mathbf{A}$ implique $a = 0$ ou $b = 0$), alors $P(\beta) = 0$ si et seulement si $\beta = \alpha$ ou $Q(\beta) = 0$. Il en résulte (par récurrence sur le degré de $P(X)$) qu'on a :

Théorème 3 *Si $(\mathbf{A},+,\cdot)$ est un anneau commutatif intègre (en particulier si c'est un corps), alors tout polynôme de degré n à coefficients dans $\mathbf{A}$ a au plus n racines dans $\mathbf{A}$.*

Exercice 4 *Montrer que $X^2-\overline{1}\in\mathbf{Z}_8[X]$ a 4 racines dans $\mathbf{Z}_8$, alors qu'il n'est que de degré 2. Y a t-il une contradiction avec le Théorème précédent?*

Exercice 5 *Rappelons que contrairement à $\mathbf{R}$ (dans lequel $X^2+1\in\mathbf{R}[X]$ n'a aucune racine), le corps $\mathbf{C}$ des nombres complexes est algébriquement clos, c'est à dire que tout polynôme non nul $P(X)\in\mathbf{C}[X]$ se factorise de manière unique sous la forme $P(X)=a(X-\lambda_1)^{e_1}\cdots(X-\lambda_n)^{e_n}$ avec les $\lambda_k\in\mathbf{C}$ deux à deux distincts. Donner toutes les racines complexes de $P(z)=z^3-1$, et en déduire la valeur de $\cos(2\pi/3)$. De même, donner toutes les racines complexes de $P(z)=z^5-1$ (remarquer que $P(z)=(z-1)(z^4+z^3+z^2+z+1)$ et que $z^4+z^3+z^2+z+1=0$ si et seulement si $(z^2+1/z^2)+(z+1/z)+1=0$, donc si et seulement si $Z=z+1/z$ est racine de $Z^2+Z-1=0$, puis Z étant connu z est racine de $z^2-Zz+1=0$) et en les situant grossièrement dans le plan complexe, en déduire que $\cos(2\pi/5)=(\sqrt{5}-1)/4$.*

Exercice 6 *(Polynôme d'interpolation de Lagrange). Soient $\lambda_1<\lambda_2<\cdots<\lambda_n$ des points donnés et a_k, $1\le k\le n$, des valeurs données, le tout dans un corps $\mathbf{K}$. Montrer qu'il existe un unique polynôme $L(X)\in\mathbf{K}[X]$ de degré $\le n-1$ tel que $L(\lambda_i)=a_i$ pour $1\le i\le n$ (i.e. il existe un unique polynôme de degré $\le n-1$ de graphe passant par n points du plan d'abcisses deux à deux distinctes), et qu'il est égal à*

$$L(X)=L_{\substack{(\lambda_1,\cdots,\lambda_n)\\(a_1,\cdots,a_n)}}(X)=\sum_{k=1}^{n}a_k\prod_{\substack{l=1\\l\neq k}}^{n}\frac{X-\lambda_l}{\lambda_k-\lambda_l}.$$

Application (factorisation dans $\mathbf{Z}[X]$ des polynômes de $\mathbf{Z}[X]$). Soit $P(X)\in\mathbf{Z}[X]$ de degré $n\ge 1$. Soit $P(X)=P_1(X)P_2(X)$ une factorisation de $P(X)$ dans $\mathbf{Z}[X]$. On peut supposer $\deg P_1(X)\le m:=[n/2]$ (partie entière). On choisit $m+1$ entiers relatifs quelconques deux à deux distincts λ_i, $1\le\lambda_i\le m+1$, et on forme la liste finie des $(m+1)$-uplets $(d_1,\cdots,d_{m+1})$ où chaque d_i est un diviseur quelconque dans $\mathbf{Z}$ de $P(\lambda_i)\in\mathbf{Z}$. Montrer que $P_1(X)$ est l'un des polynôme d'interpolation de Lagrange

$$L(X)=L_{\substack{(\lambda_1,\cdots,\lambda_{m+1})\\(d_1,\cdots,d_{m+1})}}(X),$$

de sorte qu'il suffit d'essayer un par un ces polynômes d'interpolation, de ne garder que ceux à coefficients entiers relatifs puis de voir ceux d'entre eux qui divisent $P(X)$ dans $\mathbf{Z}[X]$. Exemple : factoriser dans $\mathbf{Z}[X]$ le polynôme X^4-X^2-2 en commençant par remarquer que

$$L_{\substack{(-1,0,+1)\\(d_1,d_2,d_3)}}(X)=\frac{d_3-2d_2+d_1}{2}x^2+\frac{d_3-d_1}{2}X+d_2$$

où chaque d_i parcourt tous les diviseurs dans $\mathbf{Z}$ de $P(-1)=P(0)=P(1)=-2$ (d'où 64 tels polynômes à considérer mais dont seulement ? d'entre eux sont à coefficients dans $\mathbf{Z}$ et commençant par $\pm x^2$).

1.3 Fractions rationnelles

Soit $\mathbf{K}$ un corps, on note $\mathbf{K}(X)=\{P(X)/Q(X);\ P(X)\in\mathbf{K}[X],\ 0\neq Q(X)\in\mathbf{K}[X]\}$ l'ensemble des fractions rationnelles à coefficients dans $\mathbf{K}$. Le point important est que si $(\mathbf{K}[X],+,\cdot)$ est un anneau commutatif unitaire de groupes d'inversibles $\mathbf{K}^*=\mathbf{K}\setminus\{0\}$, donc n'est pas un corps, $(\mathbf{K}(X),+,\cdot)$ est lui un corps. Le résultat essentiel pour nous est le suivant :

Théorème 7 *(Théorème de décomposition en éléments simples sur le corps des nombres complexes). Soit $P(X)/Q(X) \in \mathbf{C}(X)$, avec*

$$Q(X) = a\prod_{k=1}^{n}(X-\lambda_k)^{e_k},$$

où les λ_k, $1 \le k \le n$, désignent les racines complexes deux à deux distinctes de $Q(X)$. Il existe alors $R(X) \in \mathbf{C}[X]$ et $a_{k,l} \in \mathbf{C}$, uniques, tels que

$$\frac{P(X)}{Q(X)} = R(X) + \sum_{k=1}^{n}\sum_{l=1}^{e_k}\frac{a_l(\lambda_k)}{(X-\lambda_k)^l}. \tag{1}$$

De plus, si $\deg P(X) < \deg Q(X)$, alors $R(X) = 0$, i.e. $R(X)$ n'apparaît pas. Par unicité, si $P(X)/Q(X) \in \mathbf{R}[X]$, alors $R(X) \in \mathbf{R}[X]$, $a_l(\lambda_k) \in \mathbf{R}$ si $\lambda_k \in \mathbf{R}$, et $a_l(\overline{\lambda_k}) = \overline{a_l(\lambda_k)}$ si $\lambda_k \in \mathbf{C}\setminus\mathbf{R}$. Finalement, on a les formules suivantes :

$$a_{e_k}(\lambda_k) = \lim_{x\to\lambda_k}(x-\lambda_k)^{e_k}\frac{P(x)}{Q(x)} = \frac{P(\lambda_k)}{a\prod_{\substack{i=1\\ i\neq k}}^{n}(\lambda_k-\lambda_i)^{e_i}}, \qquad (1 \le k \le n),$$

qui pour $e_k = 1$ (cas des racines simples de $Q(X)$) donne :

$$a_1(\lambda_k) = \lim_{x\to\lambda_k}(x-\lambda_k)\frac{P(x)}{Q(x)} = \lim_{x\to\lambda_k}\frac{P(x)}{(Q(x)-Q(\lambda_k))/(x-\lambda_k)} = \frac{P(\lambda_k)}{Q'(\lambda_k)}.$$

Dans la pratique, on écrit quelle doit être la forme de la décomposition en éléments simples, on calcule tous les $a_{e_k}(\lambda_k)$ et pour trouver les autres coefficients $a_l(\lambda_k)$, $1 \le k \le n$ et $1 \le l < e_k$, on substitue des valeurs pour X dans (1) de manière à former suffisamment d'équations linéaires en ces inconnues restantes. Donnons seulement sur un exemple des techniques permettant de rapidement trouver cette décomposition. Par exemple, il existe a, b et c complexes tels que

$$\frac{1}{(1-X)(1-X^2)} = \frac{1}{(X+1)(X-1)^2} = \frac{a}{X+1} + \frac{b}{X-1} + \frac{c}{(X-1)^2}. \tag{2}$$

Tout d'abord, a et c sont faciles à trouver. En effet, nous devons avoir

$$\frac{X+1}{(1-X)(1-X^2)} = \frac{1}{(X-1)^2} = a + b\frac{X+1}{X-1} + c\frac{X+1}{(X-1)^2},$$

qui pour la substitution $X = -1$ donne $a = 1/4$. De même, nous devons avoir

$$\frac{(X-1)^2}{(1-X)(1-X^2)} = \frac{1}{X+1} = a\frac{(X-1)^2}{X+1} + b(X-1) + c,$$

qui pour la substitution $X = 1$ donne $c = 1/2$. Finalement, la substitution $X = 0$ dans (2) donne $1 = a - b + c = 1/4 - b + 1/2$, et $b = -1/4$.

Exercice 8 *Montrer que (avec $\exp(\pm 2\pi i/3) = (-1 \pm i\sqrt{3})/2$) on a :*

$$f(X) := \frac{1}{(1-X)(1-X^3)} = \frac{-1/3}{X-1} + \frac{1/3}{(X-1)^2} + \frac{(3-i\sqrt{3})/18}{X-e^{2\pi i/3}} + \frac{(3+i\sqrt{3})/18}{X-e^{-2\pi i/3}}.$$

Application de la décomposition en éléments simples sur $\mathbf{C}$, puis sur $\mathbf{R}$, au calcul des primitives et des intégrales des fractions rationnelles $f(X) \in \mathbf{R}[X]$ (e.g. calcul de $\int 1/(x(x^2+1))$).

1.4 Séries formelles

Une série formelle à coefficients dans un anneau commutatif **A** est une expression de la forme

$$S(X) = a_0 + a_1X + a_2X^2 + \cdots = \sum_{n\geq 0} a_nX^n,$$

où contrairement au cas des polynômes on ne demande pas que la suite $(a_n)_{n\geq 0}$ à termes dans **A** soit nulle à partir d'un certain rang. On note $\mathbf{A}[[X]]$ l'ensemble des séries formelle à coefficients dans **A**, ensemble qu'on munit d'une structure d'anneau commutatif en posant $(\sum_{n\geq 0} a_nX^n) + (\sum_{n\geq 0} b_nX^n) = \sum_{n\geq 0}(a_n + b_n)X^n$ et $(\sum_{n\geq 0} a_nX^n) \cdot (\sum_{n\geq 0} b_nX^n) = \sum_{n\geq 0} c_nX^n$ avec $c_n = a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 = \sum_{k=0}^{n} a_kb_{n-k}$. Par exemple, $(1+X+X^2+X^3+X^4+\cdots)^2 = 1 + 2X + 3X^2 + 4X^3 + 5X^4 + \cdots$.

Théorème 9 *Pour $n \geq 1$ on a*

$$\frac{1}{(1-X)^n} = \sum_{m\geq 0} \binom{m+n-1}{n-1} X^m,$$

et donc pour $\lambda \neq 0$ on a

$$\frac{1}{(X-\lambda)^n} = \frac{1}{(-\lambda)^n} \frac{1}{(1-\frac{1}{\lambda}X)^n} = \sum_{m\geq 0} \frac{(-1)^n}{\lambda^{n+m}} \binom{m+n-1}{n-1} X^m.$$

Il en résulte, d'après le théorème de décomposition en éléments simples, que toutes fraction rationnelle à coefficients complexes $P(X)/Q(X)$ pour laquelle $Q(0) \neq 0$ est développable en série formelle dans $\mathbf{C}[[X]]$.

Exercice 10 *Développer en série formelle la fraction rationnelle $f(X) = 1/(1-2X\cos(\theta)+X^2)$.*

1.5 Applications arithmétiques

Exercice 11 *Montrer que $1/(1-X)(1-X^2)) = \sum_{n\geq 0} c_nX^n$ avec*

$$c_n = \frac{n+1}{2} + \frac{1+(-1)^n}{4} = \begin{cases} m+1 & \text{si } n = 2m \text{ est pair} \\ m+1 & \text{si } n = 2m+1 \text{ est impair,} \end{cases}$$

donc avec $c_n = [n/2]$ (partie entière). En déduire une formule pour le nombre de manières d'écrire un entier $n \geq 0$ sous la forme $a + 2b$ avec $a \geq 0$ et $b \geq 0$ entiers.

Exercice 12 *Développer en série formelle sur **C** la fraction rationnelle $f(X) = 1/((1-X)(1-X^3))$. On devrait trouver que $f(X) = \sum_{n\geq 0} c_nX^n$ avec $c_n = [n/3] + 1$ (partie entière). En déduire une formule pour le nombre de manières d'écrire un entier $n \geq 0$ sous la forme $a + 3b$ avec $a \geq 0$ et $b \geq 0$ entiers.*

Exercice 13 *Montrer que*

$$\frac{1}{(1-X^2)(1-X^3)} = \frac{-1/4}{X-1} + \frac{1/6}{(X-1)^2} + \frac{1/4}{X+1} + \frac{-i\sqrt{3}/9}{X-e^{2\pi i/3}} + \frac{i\sqrt{3}/9}{X-e^{-2\pi i/3}}.$$

En déduire que le nombre u_n de manières d'écrire un entier $n \geq 0$ sous la forme $2a + 3b$ avec $a \geq 0$ et $b \geq 0$ entiers vaut $\frac{n+1}{6} + \frac{1+(-1)^n}{4} + \frac{i\sqrt{3}}{9}(e^{-2\pi i(n+1)/3} - e^{2\pi i(n+1)/3})$, puis en écrivant $n = 6q + r$ avec $0 \leq r \leq 5$ montrer que $u_n = [n/6] + 1$.

Exercice 14 *Trouver une formule pour le nombre c_n de manières d'écrire un entier $n \geq 0$ sous la forme $a + 2b + 3c$ avec $a \geq 0$, $b \geq 0$ et $c \geq 0$ entiers.*

Exercice 15 *Pour a et b complexes donnés, soit $(u_n)_{n\geq 0}$ la suite à termes complexes vérifiant $u_{n+2} = au_{n+1} + bu_n$, $n \geq 0$, avec u_0 et u_1 donnés. Considérons la série formelle $S(X) = \sum_{n\geq 0} u_n X^n$. Quel est le développement en série formelle de $(A+BX+CX^2)S(X) = \sum_{n\geq 0} v_n X^n$? En déduire qu'il existe v_0 et v_1 tels que*

$$S(X) = \frac{v_0 + v_1 x}{1 - aX - bX^2},$$

donc A et B tels que

$$S(X) = \frac{A}{1 - \lambda_1 X} + \frac{B}{1 - \lambda_2 X},$$

qui donne

$$u_n = A\lambda_1^n + B\lambda_2^n,$$

où λ_1 et λ_2 sont les deux racines complexes supposées distinctes de $X^2 - aX - b$ (que se passe t-il lorsque ce polynôme a une racine double?). Donner par exemple une formule pour les termes de la suite de Fibonacci $(u_n)_{n\geq 0}$ vérifiant $u_0 = u_1 = 1$ et $u_{n+2} = u_{n+1} + u_n$, $n \geq 0$.

Exercice 16 *On suppose u_0, u_1, a et b dans un $\mathbf{Z}_m$. (i). Que deviennent les formules précédentes? (ii). Montrer que $(u_n)_{n\geq 0}$ comme ci-dessus est toujours périodique, c'est à dire qu'il existe $N \geq 0$ et $T \geq 1$ entiers tels que $u_{n+T} = u_n$ pour tout $n \geq N$ (remarquer que les couples $(u_{n+1}, u_n) \in \mathbf{Z}_m \times \mathbf{Z}_m$ ne prennent qu'un nombre fini de valeurs).*

Problème 17 *Pour $n \geq 0$ entier, on note c_n le nombre de chemins polygonaux du quadran supérieur droit à $2n$ côtés tous de pentes -1 ou $+1$ joignant le point $(0,0)$ au point $(2n,0)$, en convenant que $c_0 = 1$.*

1. *En les dessinant, montrer que $c_1 = 1$, $c_2 = 2$ et $c_3 = 5$.*
2. *Expliquer pourquoi le nombre de chemins polygonaux côtés du quadran supérieur droit à $2n$ tous de pentes -1 ou $+1$ joignant le point $(0,0)$ au point $(2n,0)$ mais ne coupant l'axe Ox qu'en $(0,0)$ et $(2n,0)$ vaut c_{n-1}.*
3. *Expliquer pourquoi le nombre de chemins polygonaux du quadran supérieur droit à $2n$ côtés tous de pentes -1 ou $+1$ joignant le point $(0,0)$ au point $(2n,0)$ mais coupant l'axe Ox au moins une fois ailleurs qu'en $(0,0)$ et $(2n,0)$ vaut $\sum_{k=1}^{n-1} c_{k-1}c_{n-k} = (\sum_{k=0}^{n-1} c_k c_{n-1-k}) - c_{n-1}$ (Noter $(2k,0)$ avec $1 \leq k \leq n-1$ le premier point de l'axe Ox en lequel le chemin coupe l'axe Ox et utiliser la question précédente).*
4. *En déduire que $c_n = \sum_{k=0}^{n-1} c_k c_{n-1-k}$, $n \geq 1$.*
5. *En déduire que $C(X) := \sum_{n\geq 0} c_n X^n$ vérifie $C(X) = 1 + XC^2(X)$.*
6. *En déduire que $C(X) = \frac{1-\sqrt{1-4X}}{2X}$, puis que*

$$c_n = \frac{1}{n+1}\binom{2n}{n}.$$

(On expliquera clairement pourquoi

$$S(X) := 1 - 2\sum_{n\geq 1} \frac{1}{n}\binom{2n-2}{n-1} X^n$$

vérifie $S^2(X) = 1 - 4X$, i.e. pourquoi $S(X) = \sqrt{1-4X}$, en calculant le développement en série formelle du produit $S(X)S(X)$. Ou bien penser aux séries de Taylor).

2 Éléments d'arithmétique

2.1 Vocabulaire

Diviseur d'un entier, nombre premier, diviseur commun à deux (ou plus) entiers, plus grand diviseur commun (pgcd) de deux (ou plus) entiers non tous nuls :

$$\mathrm{pgcd}(a,b) = \max Div(a) \cap Div(b),$$

entiers premiers entre eux, commun multiple de deux (ou plus) entiers, plus petit commun multiple (ppcm) de deux (ou plus) entiers. Division euclidienne. Plus généralement, divisibilité dans un anneau commutatif unitaire, élément irréductible.

Exercice 18 *Montrer que pour faire la liste des diviseurs $d \geq 1$ d'un entier n il suffit de savoir faire la liste de ses diviseurs $d \leq \sqrt{n}$. En déduire la liste des diviseurs $Div(72)$ et $Div(124)$ de 72 et 124, puis déterminer* $\mathrm{pgcd}(72,124)$.

Exercice 19 *Montrer que $m/\mathrm{pgcd}(m,n)$ et $n/\mathrm{pgcd}(m,n)$ sont premiers entre eux.*

Exercice 20 *Montrer que* $\mathrm{pgcd}(a+b,b) = \mathrm{pgcd}(a,b)$.

Exercice 21 *Montrer que si $a = bq + r$ alors $Div(a) \cap Div(b) = Div(b) \cap Div(r)$, qui implique* $\mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,r)$. *En déduire un algorithme (l'algorithme d'Euclide) de calcul du* pgcd *de deux entiers positifs (non tous deux nuls).*

Si on remarque seulement que dans l'algorithme d'Euclide du calcul du pgcd de deux entiers $a \geq b \geq 1$ la taille du second entier b_n des paires (a_n, b_n) avec $a_n \geq b_n \geq 1$ est strictement décroissante, on obtient que le calcul du pgcd de deux entiers $a \geq b \geq 1$ par l'algorithme d'Euclide nécessite au plus b divisions euclidiennes avant que de tomber sur un reste nul. Le Théorème suivant améliore notablement ce résultat :

Théorème 22 *Soit $c = (\log(10))/\log((1+\sqrt{5})/2) = 4.78\cdots$. Le calcul du* pgcd *de deux entiers $a \geq b \geq 0$ non tous deux nuls par l'algorithme d'Euclide nécessite au plus $1 + Cm_a$ divisions euclidiennes avant que de tomber sur un reste nul, où m_a désigne le nombre de chiffres de l'écritue de a en base* 10.

Preuve. Nous la laissons en exercice :

1. Soit $(F_n)_{n\geq 0}$ définie par récurrence par $F_0 = F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour $n \geq 0$. Montrer que
$$F_n = \frac{1}{\sqrt{5}}\left(\Big(\frac{1+\sqrt{5}}{2}\Big)^{n+1} - \Big(\frac{1-\sqrt{5}}{2}\Big)^{n+1}\right) \quad (n \geq 0)$$
et que
$$F_n \geq \Big(\frac{1+\sqrt{5}}{2}\Big)^{n-1} \quad (n \geq 1).$$
2. Montrer par récurrence sur $n \geq 1$ que si le calcul du pgcd de deux entiers $a \geq b \geq 1$ nécessite n divisions euclidiennes avant que de tomber sur un reste nul, alors $a \geq F_n$ et $b \geq F_{n-1}$.
3. Conclure (remarquer que $a \leq 10^{m_a}$). •

Exercice 23 *Soit $m > 1$ entier et a et b deux entiers non tous deux nuls. Montrer que si $a = bq + r$ alors $\mathrm{pgcd}(m^a - 1, m^b - 1) = \mathrm{pgcd}(m^b - 1, m^r - 1)$ (remarquer que $m^a - 1 = ((m^b - 1) + 1)^q m^r - 1$ est de la forme $N(m^b - 1) + (m^r - 1)$). En déduire que*

$$\mathrm{pgcd}(m^a - 1, m^b - 1) = m^{\mathrm{pgcd}(a,b)} - 1.$$

Exercice 24 *(Probabilité que deux entiers tirés au hasard soient premiers entre eux).*

1. *Montrer que $\{(m,n);\ 1 \leq m,n \leq x$ et $\mathrm{pgcd}(m,n) > 1\}$ est égal à la réunion (non disjointe) $\bigcup_{\substack{p \text{ premier} \\ 2 \leq p \leq x}} \{(m,n);\ 1 \leq m,n \leq x$ et p divise m et $n\}$. En déduire que pour $N \geq 1$ entier on a*

$$f(x) := \#\{(m,n);\ 1 \leq m,n \leq N \text{ et } \mathrm{pgcd}(m,n) = 1\} \geq cN^2$$

avec $c := 1 - \sum_{p \text{ premier}} \frac{1}{p^2} > 0$. Autrement dit, **deux entiers tirés au hasard ont une probabilité non nulle d'être premiers entre eux**.

2. *Si E est un sous-ensemble de $\mathbf{Z}$, on note 1_E sa fonction caractéristique définie par $1_E(x) = 1$ si $x \in E$ et $1_E(x) = 0$ si $x \in \mathbf{Z} \setminus E$. En particulier, si E est fini alors $\#E = \sum_{x \in \mathbf{Z}} 1_E(x)$. Si $d = p_1 \cdots p_r$ est sans facteur carré et produit de $r \geq 0$ nombres premiers deux à deux distincts, on pose $\mu(d) = (-1)^r$. Pour x réel on pose $E_d(x) := \{(m,n);\ 1 \leq m,n \leq x$ et d divise m et $n\}$ et $E(x) := \{(m,n);\ 1 \leq m,n \leq x$ et $\mathrm{pgcd}(m,n) = 1\}$.*

   (a) *Montrer par récurrence sur son nombre de facteurs premiers que si $d > 1$ est sans facteur carré alors $\sum_{\delta | d} \mu(\delta) = 0$.*

   (b) *En déduire que $\sum_{d \leq x \text{ et } d \text{ sfc}} \mu(d) 1_{E_d(x)} = 1_{E(x)}$ puis que $\#E(x) = \sum_{d \leq x \text{ et } d \text{ sfc}} \mu(d) [x/d]^2$.*

   (c) *En remarquant que $[x/d] = x/d + O(1)$ montrer que $\#E(x) = x^2 \sum_{d \leq x \text{ et } d \text{ sfc}} \frac{\mu(d)}{d^2} + O(x \log x) = cx^2 + O(x \log x)$ avec $c := \sum_{d \geq 1 \text{ et } d \text{ sfc}} \frac{\mu(d)}{d^2} > 0$*

   (on peut montrer que $c = 6/\pi^2$). Autrement dit, **deux entiers tirés au hasard ont une probabilité égale à $6/\pi^2 = 0.60792\cdots$ (donc voisine de 60%) d'être premiers entre eux**.

2.1.1 Nombres de Mersenne et de Fermat

Exercice 25 *Soit $a \geq 2$ et $n \geq 2$ entiers.*

1. *Montrer que si $a^n - 1$ est premier alors $a = 2$ et n est premier (montrer d'abord que $a = 2$ en montrant que $a - 1$ divise $a^n - 1$. Montrer ensuite que n est premier en remarquant que si $n = n_1 n_2$ avec $n_1 > 1$ et $n_2 > 1$, alors $2^{n_1} - 1$ divise $2^n - 1 = (2^{n_1})^{n_2} - 1$). Pour $n \geq 2$ l'entier*

$$M_n = 2^n - 1$$

est appelé un **nombre de Mersenne**. *Remarquer que l'Exercice 23 montre que si m et n sont premiers entre eux alors les deux nombres de Mersenne M_m et M_n sont également premiers entre eux (voir l'Exercice 91 pour une autre solution)*

2. *Montrer que si $n = a^m + 1$ est premier alors $m = 2^n$ est une puissance de 2 (remarquer que si $m = m_1 m_2$ avec $m_1 > 1$ impair, alors $a^{m_2} + 1$ divise $a^m + 1 = (a^{m_2})^{m_1} - (-1)^{m_1}$). Pour $n \geq 0$ l'entier*

$$F_n = 2^{2^n} + 1$$

est appelé un **nombre de Fermat**. *Donner des exemples montrant que $n = a^{2^n} + 1$ peut être premier sans que a soit égal à 2.*

Exercice 26 *(Application des nombres de Fermat : première minoration de $\pi(x)$. Voir également les exercices 28 et 47 pour d'autres minoration de $\pi(x)$). Posons $F_m = 2^{2^m} + 1$, $m \geq 0$ entier (nombres de Fermat). Montrer par récurrence sur $n \geq 1$ que*

$$F_n - 2 = F_0 F_1 . \cdots . F_{n-1}.$$

En déduire que les F_m, $m \geq 0$ sont deux à deux premiers entre eux (voir l'Exercice 93 pour une autre solution), puis que le nombre de nombres premiers inférieurs ou égaux à $F_n = 2^{2^n} + 1$ est supérieur ou égal à $n + 1$. En utilisant cette inégalité pour $n = \pi(x)$, montrer que le nombre $\pi(x)$ de nombre premiers inférieurs ou égaux à un réel $x \geq 3$ vérifie $x < 2^{2^{\pi(x)}} + 1$ puis

$$\pi(x) > \log_2 \log_2(x - 1),$$

où $\log_2(t) = \frac{\log t}{\log 2}$ désigne le logarithme en base 2 de $t > 0$.

2.1.2 Infinitude des nombres premiers

Théorème 27 *Il existe une infinité de nombres premiers.*

Exercice 28 *(Seconde minoration de $\pi(x)$. Voir également les exercices 26 et 47 pour d'autres minorations de $\pi(x)$). Soient $2 = p_1 < p_2 < \cdots < p_n$ les n premiers nombres premiers. En remarquant que p_{n+1} est inférieur ou égal à $1 + p_1 p_2 \cdots p_n$, montrer que pour tout $n \geq 1$ on a $p_n \leq 2^{2^{n-1}}$. En utilisant cette inégalité pour $n = \pi(x) + 1$, montrer que le nombre $\pi(x)$ de nombre premiers inférieurs ou égaux à un réel $x > 1$ vérifie*

$$\pi(x) > \log_2 \log_2(x),$$

où $\log_2(t) = \frac{\log t}{\log 2}$ désigne le logarithme en base 2 de $t > 0$.

Exercice 29

1. *Montrer qu'il existe une infinité de nombres premiers de la forme $4k + 3$ (remarquer que tout entier de la forme $4k + 3$ avec $k \geq 1$ non divisible par 3 admet au moins un diviseur premier $p > 3$ de la forme $4k + 3$, puis que si $3 < p_1 < p_2 \cdots < p_r$ sont des nombres premiers de la forme $4k + 3$, alors $n = 4p_1 . \cdots . p_r + 3$ qui est de la forme $4k + 3$ admet au moins un diviseur premier p de la forme $p = 4k + 3$ et qu'il est distinct des n précédents p_i connus).*
2. *Montrer de même qu'il existe une infinité de nombres premiers de la forme $6k + 5$.*
3. *Soit $N \geq 3$ donné. Montrer qu'il existe une infinité de nombres premiers en dehors de la progression arithmétique $\{Nk + 1;\ k \geq 1\}$ (remarquer que tout entier de la forme $Nk + N - 1$ avec $k \geq 1$ non divisible par $N - 1$ admet au moins un diviseur premier en dehors de la progression arithmétique $\{Nk + 1;\ k \geq 1\}$ et qu'il ne divise pas $N - 1$, puis que si $1 < p_1 < p_2 \cdots < p_r$ sont des nombres premiers ne divisant pas $N - 1$ et en dehors de la progression arithmétique $\{Nk + 1;\ k \geq 1\}$, alors $n = Np_1 . \cdots . p_r + N - 1$ qui est de la forme $n = Nk + N - 1$ admet donc au moins un diviseur premier p ne divisant pas $N - 1$ en dehors de la progression arithmétique $\{Nk + 1;\ k \geq 1\}$ et qu'il est distinct des p_i précédents connus). Retrouver alors les résultats des deux questions précédentes.*

Théorème 30 *(Théorème de la progression arithmétique). Si $a \geq 1$ et $b \geq 1$ sont premiers entre eux, alors la progression arithmétique $\{ak + b;\ k \geq 1\}$ contient une infinité de nombres premiers.*

Voir l'exercice 84 pour un énoncé plus faible.

2.2 Le Théorème fondamental de l'arithmétique

2.2.1 Existence de la décomposition en facteurs premiers, mais unicité?

L'existence de la décomposition en facteurs premiers de tout entier $n \geq 2$ se prouve facilement par récurrence sur $n \geq 2$ (avec l'hypothèse de récurrence H_n : tout entier k vérifiant $2 \leq k \leq n$ se décompose en facteurs premiers). L'exercice suivant montre que l'unicité n'est elle certainement pas si facile.

Exercice 31 *Posons*

$$\mathbf{A} = \{\alpha = x + 8yi;\ x \in \mathbf{Z}, y \in \mathbf{Z}\}.$$

Comme dans $\mathbf{Z}$*, on dit que* $\alpha \in \mathbf{A}$ *est "premier" si* $\alpha \neq 0$*,* 1 *et* -1 *et si* ± 1 *et* $\pm\alpha$ *sont les seuls diviseurs de* α *dans* $\mathbf{A}$*. Pour* $\alpha = x + 8yi \in \mathbf{A}$*, posons*

$$N(\alpha) = |\alpha|^2 = x^2 + 64y^2 \in \mathbf{N},$$

qu'on appelle **la norme** *de* α*. Montrer que comme* $\mathbf{Z}$ *l'ensemble* $\mathbf{A}$ *est stable par* $\pm$ *et* $\times$*, tel que les seules solutions à* $\alpha\beta = 1$ *dans* $\mathbf{A}$ *sont* $\alpha = \beta = 1$ *et* $\alpha = \beta = -1$ *(prendre les normes), que tout* $\alpha \in \mathbf{A} \setminus \{-1, 0, 1\}$ *se décompose en "facteurs premiers" (procéder comme dans* $\mathbf{Z}$ *mais en faisant ici une récurrence sur la norme de* α*). Montrer en revanche que contrairement à* $\mathbf{Z}$*, dans* $\mathbf{A}$ *on n'a pas nécessairement unicité de la décomposition en "facteurs premiers" : on a au moins deux décompositions distinctes en "facteurs premiers" suivantes de* 65 *:* $65 = 5 \cdot 13$ *et* $65 = (1 + 8i)(1 - 8i)$ *(pour montrer que* 5*,* 13*,* $1 + 8i$ *et* $1 - 8i$ *sont "premiers" on remarquera que* $z = z'z''$ *dans* $\mathbf{A}$ *implique* $N(z) = N(z')N(z'')$ *dans* $\mathbf{N}$*). Remarque :* 257 *est premier dans* $\mathbf{Z}$ *mais* $257 = 1 + 16^2 = (1 + 16i)(1 - 16i)$ *n'est pas "premier" dans* $\mathbf{A}$*.*

2.2.2 Existence et unicité de la décomposition en facteurs premiers

Structure des sous-groupes de $\mathbf{Z}$ (parties $\mathbf{G}$ de $\mathbf{Z}$ contenant 0, telles que $x \in \mathbf{G}$ implique $-x \in \mathbf{G}$, et telles que $x \in \mathbf{G}$ et $y \in \mathbf{G}$ impliquent $x + y \in \mathbf{G}$) et première preuve du Théorème de Bézout :

Proposition 32 *1. Si* $\mathbf{G}$ *est un sous-groupe de* $\mathbf{Z}$*, alors il existe un unique entier* $d \geq 0$ *tel que* $\mathbf{G} = d\mathbf{Z} := \{dx;\ x \in \mathbf{Z}\}$*.*

2. Si a *et* b *sont deux entiers non tous deux nuls alors* $\mathbf{G}_{a,b} := \{ax + by;\ x \in \mathbf{Z}, y \in \mathbf{Z}\}$ *est un sous-groupe de* $\mathbf{Z}$ *et si* $d \geq 0$ *est tel que* $\mathbf{G}_{a,b} = d\mathbf{Z}$*, alors* $d = \mathrm{pgcd}(a, b)$ *et il existe donc* $u \in \mathbf{Z}$ *et* $v \in \mathbf{Z}$ *tels que* $au - bv = \mathrm{pgcd}(a, b)$*.*

Proposition 33 *(Relation de Bézout). Pour* $a \geq 0$ *et* $b \geq 0$ *entiers non tous deux nuls, il existe* $u \geq 0$ *et* $v \geq 0$ *entiers tels que*

$$au - bv = \mathrm{pgcd}(a, b).$$

Preuve. On raisonne par récurrence sur $n = a + b \geq 2$ en remarquant que si $a = 0$ ou $b = 0$ le résultat est clair et que si $a > 0$ et $b > 0$ alors ou bien $a \geq b$, auquel cas on a $a + b > (a - b) + b$ et il existe donc $u' \geq 0$ et $v' \geq 0$ tels que $(a - b)u' - bv' = \mathrm{pgcd}(a - b, b) = \mathrm{pgcd}(a, b)$ qui donne $au - bv = \mathrm{pgcd}(a, b)$ avec $u = u' \geq 0$ et $v = u' + v' \geq 0$, ou bien $b > a$, auquel cas on a $a + b > a + (b - a)$ et il existe donc $u' \geq 0$ et $v' \geq 0$ tels que $au' - (b - a)v' = \mathrm{pgcd}(a, b - a) = \mathrm{pgcd}(a, b)$ qui donne $au - bv = \mathrm{pgcd}(a, b)$ avec $u = u' + v' \geq 0$ et $v = v' \geq 0$. •

L'algorithme d'Euclide. Soit à trouver $d = \text{pgcd}(a, b)$, le pgcd de deux entiers $a > b \geq 1$ puis u et v entiers relatifs tels que $au - bv = d$.

$\mathbf{52} = 1 \cdot \mathbf{37} + 15$
$\mathbf{37} = 2 \cdot \mathbf{15} + 7$
$\mathbf{15} = 2 \cdot \mathbf{7} + 1$
$\mathbf{7} = 7 \cdot \mathbf{1} + 0$, d'où $\text{pgcd}(52, 37) = 1$.

(on descend en utilisant des divisions euclidiennes et en remarquant que si $a_n > a_{n+1} \geq 1$ et $a_n = qa_{n+1} + a_{n+2}$ avec $0 \leq a_{n+2} < a_{n+1}$, alors $\text{pgcd}(a_n, a_{n+1}) = \text{pgcd}(a_{n+1}, a_{n+2})$ avec toujours $a_{n+1} > a_{n+2} \geq 0$).

$1 = 1 \cdot \mathbf{15} - 2 \cdot \mathbf{7}$
$1 = 1 \cdot \mathbf{15} - 2 \cdot (\mathbf{37} - 2 \cdot \mathbf{15}) = -2 \cdot \mathbf{37} + 5 \cdot \mathbf{15}$
$1 = -2 \cdot \mathbf{37} + 5 \cdot (\mathbf{52} - 1 \cdot \mathbf{37}) = 5 \cdot \mathbf{52} - 7 \cdot \mathbf{37}$

(on remonte les divisions euclidiennes précédentes).

Exercice 34 *Montrer que si d divise a et b non tous deux nuls, alors il divise* $\text{pgcd}(a, b)$.

Définition 35 *Soit* $\mathbf{A}$ *un anneau commutatif unitaire. On dit que* $D \in \mathbf{A}$ *est* **un** pgcd *de* a *et* b *de* $\mathbf{A}$ *non tous deux nuls si* D *divise* a *et* b *et si tout diviseur commun* d *à* a *et* b *divise* D. *Si* D *et* D' *sont deux* pgcd *de* a *et* b *alors il existe un inversible* $\epsilon \in \mathbf{A}^*$ *tel que* $D' = \epsilon D$ *(car* D *divse* D' *et* D' *divise* D*). Attention, un* pgcd *en ce sens n'existe pas toujours. Si* $\mathbf{A} = \mathbf{Z}$ *alors les* pgcd *en ce sens existent, et il y en a deux :* $\text{pgcd}(a, b)$ *et* $-\text{pgcd}(a, b)$ *(car* $\mathbf{Z}^* = \{\pm 1\}$*).*

Remarque 36 *Soit* k *un corps commutatif. Dans* $k[X]$ *on a également une division euclidienne, l'algorithme d'Euclide s'y applique et à nouveau il se termine par un dernier reste non nul (regarder les degrés), algorithme qui se remonte en un Bézout entre* $A(X)$, $B(X)$ *et ce dernier reste non nul* $D(X)$, *et ce* $D(X)$ *est un* pgcd *au sens précédent. Par exemple, dans* $\mathbf{Q}[X]$, *avec* $A(X) = X^3 + 1$ *et* $B(X) = X^2 + 1$, *on a successivement*

$\mathbf{X^3 + 1} = X \cdot (\mathbf{X^2 + 1}) + (-\mathbf{X + 1})$
$\mathbf{X^2 + 1} = (-X - 1) \cdot (-\mathbf{X + 1}) + \mathbf{2}$

qu'on remonte ensuite en

$\mathbf{2} = \mathbf{X^2 + 1} + (X + 1) \cdot (-\mathbf{X + 1})$
$\mathbf{2} = \mathbf{X^2 + 1} + (X+1) \cdot (\mathbf{X^3 + 1} - X \cdot (\mathbf{X^2 + 1})) = (X+1) \cdot (\mathbf{X^3 + 1}) + (-X^2 - X + 1) \cdot (\mathbf{X^2 + 1})$

Exercice 37 *Soient* $a \geq b \geq 1$ *entiers. Montrer que* $\text{pgcd}(a, b)$ *divise* $\text{pgcd}(a + b, a - b)$ *et que* $\text{pgcd}(a + b, a - b)$ *divise* $2 \times \text{pgcd}(a, b)$. *En déduire d'abord que* $\text{pgcd}(a + b, a - b) = \text{pgcd}(a, b)$ *si un seul des deux entiers* a *et* b *est impair mais que* $\text{pgcd}(a + b, a - b) = 2 \times \text{pgcd}(a, b)$ *si* a *et* b *sont tous deux impairs, puis que*

$$\text{pgcd}(a + b, a - b) = \begin{cases} \text{pgcd}(a, b) & \text{si } v_2(a) \neq v_2(b) \\ 2 \times \text{pgcd}(a, b) & \text{si } v_2(a) = v_2(b) \end{cases}$$

(où $a = 2^{v_2(a)} a'$ *avec* a' *impair et* $b = 2^{v_2(b)} b'$ *avec* b' *impair).*

Proposition 38

1. *(Lemme de Gauss). Si* a *est premier avec* b *et divise le produit* bc, *alors* a *divise* c.
2. *(Lemme d'Euclide). Si* $p \geq 2$ *premier divise un produit* $a_1 a_2 \cdots a_t$ *alors il divise l'un des* a_i.

Preuve. Preuve du Théorème de Gauss : par Bézout il existe u et v tels que $au - bv = 1$, qui donne $acu - bcv = c$ et montre que a divise c. La preuve du Lemme d'Euclide se fait par

récurrence sur $t \geq 2$, et nous ne donnons que la preuve de la première étape, pour $t = 2$. Si p ne divise pas a_1 alors p et a_1 sont premiers entre eux et le Théorème de Gauss montre que p divise a_2. •

Exercice 39 *1. Montrer que si* $\mathrm{pgcd}(a,b) > 1$ *alors il existe* $p \geq 2$ *premier divisant* a *et* b.

2. Montrer que si $\mathrm{pgcd}(a,b) = 1$ *alors pour* $k \geq 1$ *et* $l \geq 1$ *on a* $\mathrm{pgcd}(a^k, b^l) = 1$ *(utiliser le Lemme d'Euclide pour monter que si* $\mathrm{pgcd}(a^k, b^l) > 1$ *alors* $\mathrm{pgcd}(a,b) > 1$*),*

3. Montrer que si $\mathrm{pgcd}(a,b) = 1$ *alors* $\mathrm{pgcd}(a+b, ab) = 1$ *(utiliser le Lemme d'Euclide pour monter que si* $\mathrm{pgcd}(a+b, ab) > 1$ *alors* $\mathrm{pgcd}(a,b) > 1$*).*

Exercice 40 *Soit* $k \geq 2$ *fixé. Montrer que si* $uv = n^k$ *et* $\mathrm{pgcd}(u,v) = 1$*, alors il existe* n_1 *et* n_2 *premiers entre eux tels que* $n = n_1 n_2$*,* $u = n_1^k$ *et* $v = n_2^k$ *(on pourra faire une récurrence sur* $n \geq 1$ *en remarquant que si* p *premier divise* $n > 1$ *alors* p *divise* u *et est premier avec* v *(ou l'inverse), puis que* p^k *est premier avec* v *et divise* u*, et en déduire que* $u'v' = n'^k$ *avec* $u' = u/p^k$*,* $v' = v$ *et* $n' = n/p$*).*

Exercice 41 *On se propose de montrer que* $x^2 + y^2 = z^2$ *avec* $x \geq 1$*,* $y \geq 1$ *et* $z \geq 1$ *premiers dans leur ensemble (i.e.* $d \geq 1$ *divise* x*,* y *et* z *implique* $d = 1$*) si et seulement si il existe* $u \geq v \geq 1$ *premiers entre eux avec* u *ou* v *pair tels que* $\{x,y\} = \{2uv, u^2 - v^2\}$ *et* $z = u^2 + v^2$*.*

1. Montrer d'abord que si $u \geq v \geq 1$ *sont premiers entre eux alors* $x = 2uv$*,* $y = u^2 - v^2$ *et* $z = u^2 + v^2$ *sont premiers dans leur ensemble et tels que* $x^2 + y^2 = z^2$*.*

2. Réciproquement, soient $x \geq 1$*,* $y \geq 1$ *et* $z \geq 1$ *premiers dans leur ensemble tels que* $x^2 + y^2 = z^2$*.*

(a) Montrer que x*,* y *et* z *sont deux à deux premiers entre eux, que* z *est impair et que* x *ou* y *est pair et l'autre impair. Nous pouvons donc supposer* $x = 2x'$ *pair et* $x^2 + y^2 = z^2$ *s'écrit alors* $x'^2 = \frac{z+y}{2}\frac{z-y}{2}$*.*

(b) Montrer que $\mathrm{pgcd}((z+y)/2, (z-y)/2) = 1$ *et déduire de l'Exercice 40 qu'il existe* $u \geq v \geq 1$ *entiers premiers entre eux tels que* $(z+y)/2 = u^2$ *et* $(z-y)/2 = v^2$*, et que cela implique* $x = 2uv$*,* $y = u^2 - v^2$ *et* $z = u^2 + v^2$*.*

Exercice 42 *Utiliser le Lemme de Gauss pour prouver par récurrence sur* $t \geq 2$ *que si* $t \geq 2$ *entiers* $a_i \geq 1$ *deux à deux premiers entres eux divisent* n*, alors leur produit* $\prod_{i=1}^{t} a_i$ *divise* n*.*

Exercice 43 *Montrer que pour* a *et* b *non tous deux nuls et* $c \geq 1$ *on a* $\mathrm{pgcd}(ac, bc) = c \times \mathrm{pgcd}(a,b)$*.*

Exercice 44 *Montrer que si* $\mathrm{pgcd}(m_1, m_2) = 1$*, alors* $\mathrm{pgcd}(a, m_1 m_2) = \mathrm{pgcd}(a, m_1) \times \mathrm{pgcd}(a, m_2)$*.*

Exercice 45 *Utiliser le Lemme de Gauss pour montrer que*

$$\mathrm{pgcd}(a,b) \times \mathrm{ppcm}(a,b) = ab.$$

(Poser $d := \mathrm{pgcd}(a,b)$*. Montrer que* ab/d *est multiple de* a *et* b*. Réciproquement, soit* m *un multiple de* a *et* b*. En écrivant* $m = am'$ *et en utilisant lemme de Gauss, montrer que* b/d *divise* m'*, donc que* ab/d *divise* m*. D'où* $ab/d = \mathrm{ppcm}(a,b)$*).*

Théorème 46 *(Théorème fondamental de l'arithmétique). Tout entier $n \geq 2$ se factorise en un produit de nombre premiers et, à permutation près de ses termes, cette factorisation est unique (c'est à dire que si $n = p_1 \cdots p_r = q_1 \cdots q_s$ en sont deux factorisations alors $r = s$ et pour tout $i \in \{1, \cdots, r\}$ il existe $j \in \{1, \cdots, r\}$ tel que $p_i = q_j$).*

Exercice 47 *(Troisième minoration de $\pi(x)$). Soient $x \geq 2$ entier (pour simplifier) donné et $2 = p_1 < p_2 < \cdots < p_{\pi(x)} \leq x$ les nombres premiers inférieurs ou égaux à x. En remarquant que tout entier $n \leq x$ s'écrit de manière unique sous la forme $n = \prod_{k=1}^{\pi(x)} p_k^{e_k}$ et en majorant chaque e_k en fonction de x, donner un minorant explicite $f(x)$ tendant vers l'infini avec x du nombre $\pi(x)$ de nombres premiers inférieurs ou égaux à $x > 1$, et le comparer à celui obtenu aux exercices 26 et 28.*

On peut montrer :

Théorème 48 *On a $\pi(x) \sim \frac{x}{\log x}$, c'est à dire que $\lim_{x \longrightarrow \infty} \frac{\pi(x)}{x/\log x}$ existe et vaut 1.*

2.3 Le petit théorème de Fermat

Un entier relatif a est congru à un entier relatif b modulo un entier $m \geq 1$ (ce qu'on écrit $a \equiv b \pmod{m}$) si m divise la différence $b-a$. Rappelons les compatibilités de $\equiv \pmod{m}$ avec $+$ et $\times$: si $a_1 \equiv b_1 \pmod{m}$ et $a_2 \equiv b_2 \pmod{m}$ alors $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ et $a_1 a_2 \equiv b_1 b_2 \pmod{m}$. De plus, remarquons que si $n = qm + r$ alors $n \equiv r \pmod{m}$, i.e. un entier est congru modulo m à son reste dans sa division euclidienne par m.

Remarque 49 *Cette notion de congruence et ses compatibilités avec $+$ et $\times$ s'étendent au cas polynômes à coefficients dans un corps k : $A(X) \equiv B(X) \pmod{M(X)}$ si et seulement si $M(X)$ divise $B(X) - A(X)$.*

Exercice 50 *Compléter le Tableau suivant :*

Si $n \equiv$	0	1	2	3	4	5	6	(mod 7)
alors $n^2 \equiv$	?	?	?	?	?	?	?	(mod 7)
puis $n^3 \equiv$	?	?	?	?	?	?	?	(mod 7)
puis $n^4 \equiv$	?	?	?	?	?	?	?	(mod 7)
puis $n^5 \equiv$	?	?	?	?	?	?	?	(mod 7)
puis $n^6 \equiv$	?	?	?	?	?	?	?	(mod 7)
puis $n^7 \equiv$	?	?	?	?	?	?	?	(mod 7)
et $n^7 - n \equiv$	?	?	?	?	?	?	?	(mod 7)

Qu'en déduit-on? Montrer alors que pour tout $m \geq 1$ et $n \geq 0$ entiers on a $n^{m+6} \equiv n^m \pmod{7}$. La valeur de n^m modulo 7 dépend t-elle de la valeur de m modulo 6 ou de la valeur de m modulo 7? Que vaut 3^{2002} modulo 7?

Théorème 51 *(Petit théorème de Fermat). Supposons $p \geq 2$ premier. Alors, $a^p \equiv a \pmod{p}$ pour tout $a \in \mathbf{Z}$, et $a^{p-1} \equiv 1 \pmod{p}$ pour tout $a \in \mathbf{Z}$ non divisible par p. En conséquence, si pour un $N \geq 2$ il existe a non divisible par N tel que $a^{N-1} \not\equiv 1 \pmod{N}$ (et un tel a sera appelé un* **certificat de composition** *de N), alors N est composé, i.e. n'est pas premier*

Preuve. Nous la laissons en exercice :

1. Montrer que p divise chacun des coefficients binomiaux $\binom{p}{k}$ pour $1 \leq k \leq p-1$ (remarquer que $k! \times \binom{p}{k} = p \times \prod_{i=p-k+1}^{p} i$).
2. En déduire par récurrence sur $a \geq 0$ que p divise $a^p - a$ quel que soit $a \geq 0$ entier.
3. En déduire la première forme du petit théorème de Fermat : si $p \geq 2$ est premier alors p divise $a^p - a$ quel que soit a entier relatif.
4. En déduire la seconde forme du petit théorème de Fermat : si $p \geq 2$ est premier alors p divise $a^{p-1} - 1$ quel que soit a entier relatif premier à p. •

Exemple 52 *Soit* $N = F_5 = 2^{32} + 1 = 4294967297 \approx 4 \cdot 10^9$, *où* $F_n = 2^{2^n} + 1$. *Posons* $x_0 = 3$ *et* $x_m = 3^{2^m}$. *Ces* x_m *se calculent par récurrence avec la formule* $x_{m+1} = x_m^2$, *et* N *ne divise pas* $x_{32} = 3^{N-1}$ *(car* $x_{32} \equiv 3029026160 \pmod{N}$*). Il résulte du petit théorème de Fermat que* N *n'est pas premier, et on peut dire que* $a = 3$ *est un* **certificat de composition** *de* $N = F_5$. *Ce qui est surprenant, c'est qu'on peut donc certifier que* $N = F_5$ *n'est pas premier sans en donner de diviseur explicite! Il résultera de ce qui suit que pour les entiers* $N \geq 2$ *composés pour lesquels peut trouver un tel certificat de composition reposant sur l'utilisation du petit théorème de Fermat, on dispose d'un test polynomial de preuve de ce que* N *est composé ne nécessitant pas la connaissance de diviseur de* N. *Malheureusement, il existe une infinité d'entiers* $N \geq 2$ *composés (les nombres de Carmichael) n'admettant aucun certificat de composition (car vérifiant à la fois* $a^N \equiv a \pmod{N}$ *pour tout* a, *et* $a^{N-1} \equiv 1 \pmod{N}$ *pour tout* a *premier à* N*).*

Exercice 53 *En remarquant que* $2^{F_n - 1} = (F_n - 1)^{N_n}$ *avec* $N_n = 2^{2^n - n}$ *pair pour* $n \geq 1$, *montrer que* 2 *ne peut jamais être certificat de composition d'un nombre de Fermat* $F_n = 2^{2^n} + 1$ *non premier.*

2.4 Développements en base $b \geq 2$

Théorème 54 *(Écriture en base* $b \geq 2$ *de* n*). Soit* $b \geq 2$ *fixé. Pour tout entier* $n \geq 1$ *is existe* $r \geq 0$ *et des* a_i, $0 \leq i \leq r$ *vérifiant* $0 \leq a_i \leq b-1$ *pour* $0 \leq i \leq r$ *et* $a_r \neq 0$ *tels que* $n = \sum_{i=0}^{r} a_i b^i$.

Preuve. Récurrence sur n en écrivant $n = bn' + r$ avec $0 \leq r < b$. •

Exercice 55 *Écrire en bases* 2, 3 *et* 5 *l'entier qui s'écrit* 525 *en base* 10.

Exercice 56 *Effectuer (en bases* 4, 5 *et* 6*) les opérations suivantes :*

$$\begin{array}{rrr} 32123^{(4)} & 4321^{(5)} & 135^{(6)} \\ -123321^{(4)} & +1234^{(5)} & \times 531^{(6)} \end{array}$$

2.5 Calcul efficace de x^m modulo n pour m grand

Si $m = \sum_{i=0}^{r} a_i 2^i$ avec $a_i \in \{0, 1\}$, alors

$$x^m = \prod_{\substack{i=0 \\ a_k \neq 0}}^{r} x^{2^i} = \prod_{\substack{i=0 \\ a_k \neq 0}}^{r} x_i$$

où les $x_i := x^{2^i}$ vérifient $x_{i+1} = x^{2^{i+1}} = x^{2 \cdot 2^i} = (x^{2^i})^2 = x_i^2$ et $x_0 = 1$. On en déduit l'algorithme suivant de calcul efficace de x^m modulo $n \geq 2$:

Algorithme 57

1. *Poser* $e = m$, $prod = 1$, $x_i = 1$ *et* $x = x$ *modulo* n.

2. *Si $e = 0$ alors aller à l'étape 4*
3. *Si e est pair, faire $x_i = x_i^2$ modulo n, $e = e/2$ et aller à l'étape 2. Sinon, e est impair, et faire $prod = prod \times x_i$ modulo n, $x_i = x_i^2$ modulo n, $e = (e-1)/2$ et aller à l'étape 2.*
4. *Imprimer $prod$, qui est égal à x^m modulo n.*

Remarquer qu'on doit faire au plus $2r$ multiplications modulo n d'entiers $\leq n$ et au plus $2r$ divisions euclidiennes par n d'entiers $\leq n^2$ pour faire ce calcul. Puisque $a_r \neq 0$ donne $m \geq 2^r$ et $r \leq \log_2 m$, on a donc un algorithme polynomial de calcul de x^m modulo n.

Exercice 58 *Écrire en base 2 l'entier qui s'écrit 53 en base 10. Posons alors $x_m = 2^{2^m}$. Que vaut x_0? Exprimer x_{m+1} en fonction de x_m. En déduire que $2^{53} = x_0x_2x_4x_5$. En complétant le tableau suivant :*

$$\begin{array}{rcccccc} m = & 0 & 1 & 2 & 3 & 4 & 5 \\ x_m \equiv & ? & ? & ? & ? & ? & ? \end{array} \pmod{107}$$

déterminer 2^{53} modulo 107 (c'est à dire, déterminer $r \in \{0, 1, 2, \cdots 105, 106\}$ tel que $2^{53} \equiv r \pmod{107}$).

Exercice 59 *Soit $(F_n)_{n\geq 0}$ définie par $F_0 = F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour $n \geq 0$. Soit*

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Montrer que

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = A^n \begin{pmatrix} F_1 \\ F_0 \end{pmatrix}$$

et en déduire un algorithme efficace de calcul de F_n modulo m. Que vaut F_{1024} modulo 101 (réponse : 83)? (Voir également l'Exercice 87).

3 Calculs modulaires et classes de congruences

Définition du symbole $a \equiv b \pmod m$, compatibilité de $\equiv \pmod m$ avec l'addition et la multiplication.

Exercice 60 *Montrer que le dernier chiffre dans l'écriture en base* 10 *de* $F_n = 2^{2^n} + 1$, $n \geq 2$ *vaut* 7, *c'est à dire que* $2^{2^n} \equiv 6 \pmod{10}$ *(commencer par montrer que* 2^m *modulo* 10 *ne dépend que de* $m \geq 1$ *modulo* 4, *puis remarquer que* $m = 2^n \equiv 0 \pmod 4$ *pour* $n \geq 2$*).*

Exercice 61 *On définit les puisances itérées* $a^{(n)}$ *de* a *par* $a^{(1)} = a$, $a^{(2)} = a^a$, $a^{(3)} = a^{(a^a)}$ *et* $a^{(n+1)} = a^{a^{(n)}}$. *Déterminer* $7^{(2004)}$ *modulo* 11 *(commencer par montrer que* 7^n *modulo* 11 *ne dépend que de* n *modulo* 10, *puis montrer que* $n = 7^m$ *modulo* 10 *ne dépend que de* m *modulo* 4, *puis finalement remarquer que si* $m = 7^k$ *avec* k *impair, alors* $m \equiv (-1)^k \equiv -1 \equiv 3 \pmod 4$*).*

3.1 Le théorème chinois des restes

Exercice 62 *Soient* $d_1 \geq 1$ *et* $d_2 \geq 1$ *premiers entre eux. Montrer que le système de congruences*

$$\begin{cases} x \equiv x_1 \pmod{d_1} \\ x \equiv x_2 \pmod{d_2} \end{cases}$$

admet une unique solution x *modulo* $d_1 d_2$. *Application : résoudre le système de congruences*

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 5 \pmod{25} \end{cases}$$

puis le système de congruences

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 5 \pmod{25} \\ x \equiv 1 \pmod{77} \end{cases}$$

Théorème 63 *(***Théorème chinois des restes***). Soient* d_i, $1 \leq i \leq r$, *des entiers deux à deux premiers entre eux. Alors, quels que soient les* x_i, $1 \leq i \leq r$, *il existe* x *unique modulo* $d := \prod_{i=1}^r d_i$ *tel que* $x \equiv x_i \pmod{d_i}$ *pour* $1 \leq i \leq r$. *Si* $1 \equiv v_i d/d_i \pmod{d_i}$ *(Bézout, en remarquant que* $\mathrm{pgcd}(d_i, d/d_i) = 1$*), on peut prendre* $x = \sum_{i=1}^r x_i v_i d/d_i$.

Exercice 64 *Soient* $d_1 \geq 1$ *et* $d_2 \geq 1$ *non nécessairement premiers entre eux. Montrer que la congruence*

$$\begin{cases} x \equiv x_1 \pmod{d_1} \\ x \equiv x_2 \pmod{d_2} \end{cases}$$

admet au moins une solution x *si et seulement si* $x_1 \equiv x_2 \pmod{\mathrm{pgcd}(d_1, d_2)}$.

Exercice 65 *On se propose de prouver la généralisation suivante du théorème chinois des restes : soient* $d_1 \geq 1, \cdots, d_r \geq 1$ *des entiers non nuls et soient* $x_1, \cdots, x_r$ *des entiers relatifs donnés. Il existe au moins un entier relatif* x *vérifiant le système de congruences*

$$\begin{cases} x \equiv x_i \pmod{d_i} \\ 1 \leq i \leq r \end{cases}$$

si et seulement

$$\begin{cases} x_i \equiv x_j \pmod{\mathrm{pgcd}(d_i, d_j)} \\ 1 \leq i, j \leq r. \end{cases}$$

1. *Montrer que cette condition est effectivement nécessaire.*

2. *Réciproquement, on suppose maintenant que cette condition nécessaire est satisfaite. On note $\mathcal{P}$ l'ensemble des diviseurs premiers distincts du produit $\prod_{i=1}^{r} d_i$.*

   (a) *Montrer que*

$$\begin{cases} x \equiv x_i \pmod{d_i} \\ 1 \leq i \leq r \end{cases} \iff \begin{cases} x \equiv x_i \pmod{p^{v_p(d_i)}} \\ 1 \leq i \leq r,\ p \in \mathcal{P} \end{cases}$$

   (b) *Montrer que pour chaque $p \in \mathcal{P}$ on a*

$$\begin{cases} x \equiv x_i \pmod{p^{v_p(d_i)}} \\ 1 \leq i \leq r \end{cases} \iff x \equiv x_{i(p)} \pmod{p^{v_p(d_i(p))}}$$

   où $i(p) \in \{1, \cdots, r\}$ est tel que $v_p(d_{i(p)}) = \max_{1 \leq i \leq r} v_p(d_i)$ (utiliser la condition nécessaire supposée satisfaite).

   (c) *Montrer que*

$$\begin{cases} x \equiv x_i \pmod{d_i} \\ 1 \leq i \leq r \end{cases} \iff \begin{cases} x \equiv x_{i(p)} \pmod{p^{v_p(d_{i(p)})}} \\ p \in \mathcal{P} \end{cases}$$

   (d) *Conclure (en utilisant le théorème chinois des restes ordinaire).*

3.2 Définition des classes de congruence

Soit $m \geq 1$ un entier strictement positif. On définit la **classe de congruence** d'un entier relatif a modulo m, notée $[a]_m$, comme étant la progression arithmétique $a + m\mathbf{Z}$, c'est à dire que

$$[a]_m = \{a + km;\ k \in \mathbf{Z}\} = \{n \in \mathbf{Z};\ n \equiv a \pmod{n}\}.$$

Il est facile de voir que pour tout $a' \in [a]_m = a + m\mathbf{Z}$ on a $[a']_m = [a]_m$, ce qu'on traduit en disant que tout élément d'une classe de congruence en est un **représentant**, et toute classe de congruence admet donc une infinité de représentants. De plus, quels que soient les entiers relatifs a et b, on a

$$[b]_m = [a]_m \iff b \equiv a \pmod{m},$$

c'est à dire si et seulement si m divise $b - a$. Si chaque classe de congruence admet une infinité de représentants, il n'y a en revanche qu'un nombre fini de classes de congruence modulo $m \geq 1$. Plus précisément, il est facile de voir qu'il y a précisément m classes de congruence modulo m, à savoir les m classes $[0]_m$, $[1]_m$, $\cdots$, $[m-1]_m$. On note $\mathbf{Z}_m$ (ou quelquefois $\mathbf{Z}/m\mathbf{Z}$) l'ensemble $\{[0]_m, [1]_m, \cdots, [m-1]_m\}$ des m classes de congruence modulo m. On définit alors deux opérations $+$ et $\cdot$ sur $\mathbf{Z}_m$:

l'addition : $[a]_m + [b]_m = [a+b]_m$

la multiplication : $[a]_m \cdot [b]_m = [ab]_m$

Il faut bien comprendre qu'il y a un petit travail à faire pour voir que ces opérations sont effectivement bien définies. En effet, on dit (par exemple) que pour définir la somme de deux classes de congruences $\mathcal{C}_1$ et $\mathcal{C}_2$ on choisit un représentant $a \in \mathcal{C}_1$ et un représentant $b \in \mathcal{C}_2$ et que la classe somme $\mathcal{C}_1 + \mathcal{C}_2$ est définie comme étant la classe $[a+b]_m$ de la somme de ces représentants. Il faut donc vérifier que si on choisit d'autres représentants $a' \in \mathcal{C}_1$ et $b' \in \mathcal{C}_2$ pour ces classes, alors $[a'+b']_m = [a+b]_m$. Par exemple, $a = 2$ et $a' = -8$ sont deux représentants de $[2]_5$, $b = 3$ et $b' = 8$ sont deux représentants de $[3]_5$, et on a bien que $[a+b]_5 = [2+3]_5 = [-8+8] = [a'+b']_5$, car $[5]_5 = [0]_5$ puisque $5 \equiv 0 \pmod{5}$.

Ces définitions sont un peu analogues à la manière dont on définit un rationnel et l'addition et la multiplication de deux rationnels. On représente un rationnel $x \in \mathbf{Q}$ par des fractions m/n avec $m \in \mathbf{Z}$ et $n \in \mathbf{Z}$ non nul, mais un même rationnel admet une infinité de repésentants

(e.g. $2 = 2/1 = 4/2 \cdots = (2k)/k$). Plus précisément, on dit que deux fractions m/n et m'/n' représentent un même rationnel si elles vérifient $mn' = m'n$ et un rationnel est un classe de fractions. On définit alors la somme de deux rationnels x_1 et x_2 représentés par des fractions m_1/n_1 et m_2/n_2 comme étant le rationnel repésenté par la fraction $(m_1n_2 + m_2n_1)/(n_1n_2)$. Ici encore, pour voir que cette opération sur les rationnels est bien définie, il faut voir que le résultat ne dépend pas des fractions qu'on choisit pour représenter ces rationnels. Il faut donc vérifier que si on choisit d'autres représentants m_1'/n_1' et m_2'/n_2' pour ces rationnels, alors les deux fractions $(m_1n_2 + m_2n_1)/(n_1n_2)$ et $(m_1'n_2' + m_2'n_1')/(n_1'n_2')$ représentent le même rationnel. Par exemple, les deux fractions $4/3$ et $20/15$ représentent un même rationnel x_1 et les deux fractions $(-1)/2$ et $2/(-4)$ représentent un même rationnel x_2, et on a bien que les deux fractions $5/6 = 4/3+(-1)/2$ et $(-50)/(-60) = 20/15 + 2/(-4)$ représentent un même rationnel.

Exercice 66 *Montrer que les classes $[0]_m$ et $[1]_m$ vérifient $[0]_m+[a]_m = [a_m]$, $[0]_m\cdot[a]_m = [0]$ et $[1]_m\cdot[a]_m = [a_m]$ quelle que soit la classe $[a]_m$. Autrement dit, $[0]_m$ et $[1]_m$ jouent pour l'addition et la multiplication dans $\mathbf{Z}_m$ les mêmes rôles que 0 et 1 pour l'addition et la multiplication dans $\mathbf{Z}$. Une classe $[a]_m$ est dite* **inversible** *si il existe une classe $[b]_m$ telle que $[a]_m \cdot [b]_m = [1]_m$, cette classe $[b]_m$ étant alors appelée son* **inverse** *et notée $[a_m]^{-1}$ (on notera qu'il n'y a aucune ambiguïté car on montrera que si $[a]_m$ est inversible et $[a]_m \cdot [b]_m = [1]_m = [a]_m \cdot [b']_m$ alors $[b]_m = [b']_m$). Dresser les tables d'addition et de multiplication dans $\mathbf{Z}_4$ et $\mathbf{Z}_5$, puis faire des observations (donner la liste des inversibles, $\cdots$).*

Exercice 67 *Montrer que $[a]_m \in \mathbf{Z}_m$ est inversible si et seulement si a est premier à m et que si $au - mv = 1$ (Bézout), alors $[a]_m$ est d'inverse $[u]_m$. En déduire que $[77]_{102} \in \mathbf{Z}_{102}$ est inversible et donner son inverse.*

3.3 Groupes, anneaux commutatifs unitaires et leurs groupes d'unités

Vocabulaire : loi de composition interne, élément neutre, groupe, ordre d'un groupe.

Exercice 68 *Montrer que si $*$ est une loi de composition interne sur G alors G a au plus un élément neutre pour $*$.*

Exercice 69 *Soit $G :=]-c, c[\subseteq \mathbf{R}$ (avec $c > 0$) muni de la loi*

$$u \star v = \frac{u+v}{1+\frac{uv}{c^2}}$$

(loi d'addition relativiste des vitesses). Montrer que $(G, \star)$ est un groupe commutatif.

Théorème 70 *Les sous-groupes du groupe additif $(\mathbf{Z}, +)$ sont les $d\mathbf{Z} = \{dk;\ k \in \mathbf{Z}\}$ avec $d \geq 0$. (Applications au* pgcd *et à Bézout).*

Vocabulaire : anneau, anneaux commutatif unitaire, élément inversible, groupe des unités $\mathbf{A}^*$ d'un anneau commutatif unitaire $\mathbf{A}$, corps commutatif (=anneau commutatif unitaire $\mathbf{A}$ pour lequel $\mathbf{A}^* = \mathbf{A} \setminus \{0\}$), anneau intègre ($ab = 0$ implique $a = 0$ ou $b = 0$. Par exemple, $(\mathbf{Z}_4, +, \cdot)$ n'est pas un anneau intègre puisque $a = b = [2]_4 \neq 0$ mais $ab = [4]_4 = [0]_4$). Soit $(\mathbf{A}, +, \cdot)$ un anneau commutatif unitaire. On dit que $(\mathbf{A}, +, \cdot)$ est un corps si $\mathbf{A}^* = \mathbf{A} \setminus \{0_A\}$, c'est -à-dire si tout élément non nul de $\mathbf{A}$ est inversible dans $\mathbf{A}$. Par exemple, $(\mathbf{Z}_4, +, \cdot)$ n'est pas un corps puisque $[2]_4$ n'est pas inversible dans $\mathbf{Z}_8$.

Exercice 71 *Déterminer les groupes des unités des anneaux commutatifs unitaires suivants : $\mathbf{Z}$, $\mathbf{D} = \{m/10^n;\ m \in \mathbf{Z},\ n \geq 0\}$, $\mathbf{Z}[X]$, $\mathbf{Q}[X]$, $\mathbf{Z}_7$ et $\mathbf{Z}_8$.*

Exercice 72 *Montrer qu'un corps est un anneau intègre, c'est à dire que dans un corps un produit de deux éléments est nul si et seulement si un au moins d'entre eux est nul.*

Exercice 73 *Montrer que pour $m \geq 2$ l'anneau $(\mathbf{Z}_m, +, \cdot)$ est intègre si et seulement si m est premier (si $m > 1$ n'est pas premier et $1 < d < m$ est un diviseur propre de m, on remarquera que $1 < m/d < m$ et $[d]_m \cdot [m/d]_m = [0]_m$).*

Exercice 74 *Montrer par récurrence sur le nombre de diviseurs premiers $\omega(m)$ de $m > 1$ que pour tout $N \geq 1$ divisible par m on a*

$$\#\{k;\ 1 \leq k \leq N \text{ et } \mathrm{pgcd}(k, m) = 1\} = N \prod_{p|m} (1 - \frac{1}{p}).$$

Théorème 75 *Soit $m \geq 2$ entier. L'ensemble fini $\mathbf{Z}_m$ de cardinal m des classes de congruence modulo m muni des lois de compositions internes $+$ et $\times$ précédemment définies forme un anneau commutatif unitaire de neutres $[0]_m$ pour $+$ et $[1]_m$ pour $\times$. De plus $[a]_m \in \mathbf{Z}_m^*$ si et seulement si a est premier à m, auquel cas l'inverse $[a]_m^{-1}$ de $[a]_m$ est $[u]_m$ où $au - vm = 1$ (Bézout) Le groupe multiplicatif $(\mathbf{Z}_m^*, \times)$ est donc d'ordre*

$$\phi(m) := \#\{k;\ 1 \leq k \leq m \text{ et } \mathrm{pgcd}(k, m) = 1\}$$

et l'anneau $(\mathbf{Z}_m, +, \times)$ est un corps si et seulement si m est premier. Finalement,

$$\phi(m) = m \prod_{p|m} (1 - \frac{1}{p}).$$

En conséquence, $m \geq 2$ est premier si et seulement si le groupe multiplicatif $\mathbf{Z}_m^*$ est d'ordre $m - 1$.

Exercice 76 *Soit $p \geq 3$ premier. Montrer que si $p \geq 3$ est premier alors les seuls $g \in \mathbf{Z}_p^*$ vérifiant $g^2 = 1$ sont $g = 1$ et $g = -1 = p - 1$. En regroupant alors dans le produit*

$$\prod_{g \in \mathbf{Z}_p^* \setminus \{1, -1\}} g$$

(calculé dans le groupe multiplicatif $(\mathbf{Z}_p^*, \cdot)$) les éléments par paires (g, g^{-1}), montrer que ce produit est égal à 1, en déduire le théorème de Wilson : si $p \geq 3$ est premier impair, alors

$$(p - 1)! \equiv -1 \pmod{p}.$$

(voir l'Exercice 79 pour une autre solution). Montrer finalement que si $n > 4$ n'est pas premier alors $(n - 1)! \equiv 0 \pmod{n}$.

Exercice 77 *Trouver tous les $g \in \mathbf{Z}_8$ tels que $g^2 = 1$ et toutes les $A \in M_2(\mathbf{R})$ telle que $A^2 = I_2$.*

Exercice 78

1. *Montrer (en l'évaluant sur les 8 élements de $\mathbf{Z}_8$) que le polynôme $x^2 - 1 \in \mathbf{Z}_8[x]$ a 4 racines dans $\mathbf{Z}_8$.*
2. *Trouver toutes les racines de $P(x) = x^2 - 1$ dans $\mathbf{Z}_n$ avec $n = 60 = 4 \cdot 3 \cdot 5$ (remarquer que $P([a]_n) = 0$ si et seulement si $a = 2b + 1$ est impair et $3 \cdot 5$ divise $b(b + 1)$. Réponse : $x \in \{\pm 1, \pm 11, \pm 19, \pm 29\}$.*

3. *Soient* $\mathbf{A}$ *un anneau,* $P(x)=\sum_{k=0}^{d} p_k x^k \in \mathbf{A}[x]$ *de degré* $d\geq 1$ *et* $a\in\mathbf{A}$ *tel que* $P(a)=0$. *Montrer qu'il existe* $Q(x)\in\mathbf{A}[x]$ *de degré* $d-1$ *tel que*

$$P(x)=(x-a)Q(x)$$

(remarquer que $P(x)=P(x)-P(a)=\sum_{k=1}^{d} p_k(x^k-a^k)$*).*

4. *Utiliser la question précédente pour prouver par récurrence sur* $d\geq 1$ *qu'un polynôme de degré* $d\geq 1$ *à coefficients dans un corps* $\mathbf{K}$ *possède au plus* d *racines dans* $\mathbf{K}$. *Remarquer que les deux premières questions montrent que le résultat peut être faux pour des polynômes qui ne sont pas à coefficients dans un corps.*

Exercice 79 *Soit* $p\geq 3$ *premier. Montrer que*

$$X^{p-1}-1=\prod_{a=1}^{p-1}(X-[a]_p)$$

dans $\mathbf{Z}_p[X]$, *puis en déduire le théorème de Wilson :*

$$(p-1)!\equiv -1 \pmod p$$

(voir l'Exercice 76 pour une autre solution).

Exercice 80 *Soit* $p\geq 2$ *premier. Montrer que* $P(X)=X^n+\sum_{k=0}^{n-1} a_k X^k\in\mathbf{Z}_p[X]$ *unitaire a au moins une racine dans* $\mathbf{Z}_p$ *si et seulement si*

$$\deg(\mathrm{pgcd}(X^p-X,P(X)))\geq 1.$$

En déduire pour $P(X)\in\mathbf{Z}[X]$ *fixé unitaire de degré* $n\geq 1$, *un algorithme testant pour* p *premier variable l'existence d'un* $n\in\mathbf{Z}$ *tel que* $P(n)\equiv 0 \pmod p$.

Exercice 81 *Pour* $d\in\mathbf{Z}$ *non carré parfait on pose*

$$\mathbf{Z}[\sqrt{d}]=\{x+y\sqrt{d};\ x\in\mathbf{Z},\ y\in\mathbf{Z}\}.$$

Pour $\alpha=x+y\sqrt{d}\in\mathbf{Z}[\sqrt{d}]$ *on pose* $\alpha'=x-y\sqrt{d}$ *et*

$$N(\alpha):=\alpha\alpha'=x^2-dy^2\in\mathbf{Z}.$$

Montrer que α *est une unité de* $\mathbf{Z}[\sqrt{d}]$ *si et seulement si* $N(\alpha)=\pm 1$. *En déduire le groupe des unités des anneaux* $\mathbf{Z}[\sqrt{d}]$ *pour* $d<0$. *Montrer que* $\epsilon_0=1+\sqrt{2}$ *est une unité de* $\mathbf{Z}[\sqrt{2}]$*; montrer que pour toute unité* $\epsilon\neq\pm 1$ *de* $\mathbf{Z}[\sqrt{2}]$ *un seul* η *des quatre éléments* $\pm\epsilon$, $\pm 1/\epsilon$ *est* >1 *et qu'il est alors de la forme* ϵ_0^m *pour un* $m\geq 1$ *entier (poser* $m=\max\{k\geq 1;\epsilon_0^k\leq\eta\}$*); et en déduire que le groupe des unités de l'anneau* $\mathbf{Z}[\sqrt{2}]$ *est égal à* $\{\pm\epsilon_0^m;\ m\in\mathbf{Z}\}$. *Il est en particulier infini.*

Soit $\mathbf{A}$ un anneau commutatif unitaire et $\mathbf{I}$ un idéal de $\mathbf{A}$. Comme au paragraphe 3.2, l'ensemble quotient $\mathbf{A}/\mathbf{I}$ des classes de congruence modulo $\mathbf{I}$, c'est à dire l'ensemble des $[a]_{\mathbf{I}}=a+\mathbf{I}=\{a+i;\ i\in\mathbf{I}\}$ est canoniquement muni d'une structure d'anneau et on note $(\mathbf{A}/\mathbf{I})^*$ le groupe des éléments inversibles de l'anneau quotient $\mathbf{A}/\mathbf{I}$, où une classe $[a]_{\mathbf{I}}$ est dite inversible si il existe $[a']_{\mathbf{I}}$ telle que $[a]_{\mathbf{I}}\cdot[a']_{\mathbf{I}}=[1]_{\mathbf{I}}$.

Exercice 82 *Soient* $d\in\mathbf{Z}$ *non carré,* $\mathbf{A}=\mathbf{Z}[\sqrt{d}]$ *et* p *premier. Montrer que* $\alpha=x+y\sqrt{d}\in(\mathbf{A}/p\mathbf{A})^*$ *si et seulement si* p *ne divise pas*

$$N(\alpha)=x^2-dy^2\in\mathbf{Z}.$$

En déduire que le groupe $(\mathbf{A}/p\mathbf{A})^*$ *est d'ordre* p^2-1 *si la congruence* $x^2\equiv d \pmod p$ *n'a pas de solution* $x\in\mathbf{Z}$, *d'ordre* $p(p-1)$ *si* p *divise* d *et est d'ordre* $(p-1)^2$ *si* p *ne divise pas* d *et si la congruence* $x^2\equiv d \pmod p$ *a au moins une solution* $x\in\mathbf{Z}$.

Exercice 83 *Soient A un anneau commutatif, I et J deux idéaux de A et x_I et x_J deux éléments de A. Montrer que $I+J := \{i+j;\ i \in I,\ j \in J\}$ est un idéal de A et que le système d'équations*

$$\begin{cases} x \equiv x_I \pmod{I} \\ x \equiv x_J \pmod{J} \end{cases}$$

admet au moins une solution si et seulement si $x_I - x_J \in I + J$ (si $x_I - x_J = i + j$, prendre $x = x_I - i = y_J + j$). Montrer que le résultat de l'exercice 65 n'est qu'un cas particulier de celui-ci.

Exercice 84 *Si $a \geq 1$ et $b \geq 1$ sont premiers entre eux et si $n \geq 1$ est donné, alors la progression arithmétique $\{ak+b;\ k \geq 0\}$ contient une infinité de nombres premiers à n. On commencera par montrer qu'on peut écrire $n = n_1 n_2$ avec $n_1 \geq 1$ tel que p divise n_1 implique p divise a, et $n_2 \geq 1$ premier à a. On montrera alors que $ak + b$ est premier à n si et seulement si il est premier à n_2. On en déduira qu'il existe $\phi(n_2)$ entiers $k_i \in \{0, \cdots, n_2 - 1\}$ tels que $ak + b$ est premier à n si et seulement si k appartient à la réunion des progressions arithmétiques $\{n_2 l + k_i;\ l \geq 0\}$.*

4 Groupes abéliens finis

Vocabulaire : ordre d'un groupe, groupe monogène, groupe cyclique, générateur d'un groupe, sous-groupe.

Exercice 85 *Soit G un groupe abélien fini d'ordre pair $2n \geq 1$ et contenant un sous-groupe H d'ordre n. Montrer que pour $g \in G \setminus H$ l'application $h \in H \mapsto gh \in G \setminus H$ est définie et bijective. En déduire que pour tout $g \in G$ on a $g^2 \in H$.*

4.1 Ordre d'un élément dans un groupe

Théorème 86 *Soit G un groupe abélien fini d'ordre $n \geq 1$.*

1. *Quel que soit $g \in G$ l'entier*
$$\text{ordre}(g) := \min\{k \geq 1;\ g^k = 1_G\}$$
*est bien défini et est appelé l'***ordre** *de g dans le abélien fini G.*
2. *Pour $m \geq 0$ entier on a*
$$g^m = 1_G \Longleftrightarrow \text{ordre}(g) \text{ divise } m.$$
3. *Pour tout $g \in G$ on a $g^n = 1_G$.*
4. *En conséquence, l'ordre de tout élément d'un groupe abélien fini G divise l'ordre de G.*

Preuve. Nous la laissons en exercice :

1. Montrer que deux des éléments de l'ensemble $\{1_G = g^0, g^1, g^2, \cdots, g^n\}$ sont égaux.
2. Montrer que si $a > b \geq 0$ et $g^a = g^b$ alors $g^{a-b} = 1_G$.
3. En déduire que $\text{ordre}(g) := \min\{k \geq 1;\ g^k = 1_G\}$ est bien défini.
4. Soit $m \geq 1$. Écrire $m = q \times \text{ordre}(g) + r$ avec $0 \leq r < \text{ordre}(g)$ pour voir que $g^m = 1_G$ si et seulement si $g^r = 1_G$, donc si et seulement si $r = 0$.
5. Soit $\Pi_G := \prod_{h \in G} h$ (=produit de tous les éléments de G). En remarquant que $h \in G \mapsto gh \in G$ est une bijection de G dans G, montrer que $\Pi_G = g^n \Pi_G$, puis que $g^n = 1_G$. •

Exercice 87 *(En lien avec le point 1. de la preuve du Théorème 22 et l'Exercice 59). Soit $\rho = [56]_{101}$ ou $\rho = [45]_{101}$ l'une quelconque des deux racines carrées de $[5]_{101}$ dans le groupe multiplicatif $(\mathbf{Z}_{101}^*, \cdot)$ d'ordre 100. Posons $\alpha_+ = ([1]_{101} + \rho)/[2]_{101}$ et $\alpha_- = ([1]_{101} - \rho)/[2]_{101}$. Montrer par récurrence sur $n \geq 0$ que si $F_0 = F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour $n \geq 0$ (suite de Fibonacci) alors*
$$[F_n]_{101} = \frac{1}{\rho}\Big(\alpha_+^{n+1} - \alpha_-^{n+1}\Big), \quad n \geq 0.$$
En déduire que si
$$d = \text{ppcm}(\text{ordre}_{\mathbf{Z}_{101}^*}(\alpha_+), \text{ordre}_{\mathbf{Z}_{101}^*}(\alpha_-)),$$
alors la suite $(F_n)_{n \geq 0}$ modulo 101 est purement périodique de période $d \geq 0$ et que 101 divise F_n pour $n \equiv -1 \pmod{d}$. Choisissons $\rho = [56]_{101}$. Alors, $\alpha_+ = ([1]_{101} + \rho)/[2]_{101} = [79]_{101}$ est d'ordre 25 et $\alpha_- = ([1]_{101} - \rho)/[2]_{101} = [23]_{101}$ est d'ordre 50. Donc $d = 50$. En déduire que $F_{1024} \equiv 83 \pmod{101}$.

Exercice 88 *Soit $(G,\cdot)$ un groupe multiplicatif commutatif de neutre 1_G.*

1. *Si $g \in G$ est d'ordre n dans G et si $\mathrm{pgcd}(m,n)=1$, alors g^m est d'ordre n dans G.*
2. *Si $g \in G$ est d'ordre n dans G et si $d \geq 1$ divise n, alors g^d est d'ordre n/d dans G.*
3. *En utilisant les deux questions précédentes, montrer que si $g \in G$ est d'ordre n dans G, alors g^m est d'ordre $n/\mathrm{pgcd}(m,n)$ dans G.*
4. *Si $g_1 \in G$ est d'ordre n_1 dans G, si $g_2 \in G$ est d'ordre n_2 dans G et si $\mathrm{pgcd}(n_1,n_2)=1$, alors $g=g_1g_2$ est d'ordre $n=n_1n_2$ dans G.*
5. *En déduire pour des $g_i \in G$, $1 \leq i \leq k$, d'ordres respectifs n_i, $1 \leq i \leq k$, la construction d'un élément $g \in G$ d'ordre $n = \mathrm{ppcm}(n_1,\cdots,n_k)$ (on pourra faire une récurrence sur $k \geq 2$).*

Exercice 89 *Montrer que pour $n>1$ et a premier à n, $[a]_n^{\phi(n)-1}$ est l'inverse de $[a]_n$ dans $\mathbf{Z}_n^*$. En utilisant l'algorithme 57, en déduire un algorithme efficace de calcul de Bézout effectif de u et v tels que $xu-nv=1$. Exemple : en donnant la table des $x_i := [73]_{132}^{2^i}$ pour $0 \leq i \leq 5$, calculer $[73]_{132}^{-1}$ puis u et v tels que $73u-132v=1$.*

Exercice 90 *Soit $M_p = 2^p-1$ un nombre de Mersenne avec p premier. Montrer que si $q \geq 3$ non nécessairement premier divise M_p alors $g=[2]_q$ est d'ordre p dans le groupe $G=\mathbf{Z}_q^*$. En déduire que si $q \geq 3$ premier divise M_p alors*

$$q \equiv 1 \pmod{2p}.$$

Exercice 91 *Soit $l \geq 3$ premier divisant deux nombres de Mersenne $M_m = 2^m-1$ et $M_n = 2^n-1$ avec $m \geq 2$ et $n \geq 2$ non nécessairement premiers. En remarquant que l'ordre de $g=[2]_l$ dans le groupe $G=\mathbf{Z}_l^*$ divise m et n, montrer que $\mathrm{pgcd}(m,n)>1$. Autrement dit, si m et n sont premiers entre eux alors les deux nombres de Mersenne M_m et M_n sont également premiers entre eux (voir l'Exercice 23 pour une autre solution).*

Exercice 92 *Soit $F_m = 2^{2^m}+1$ un nombre de Fermat. Montrer que si $q \geq 3$ non nécessairement premier divise F_m alors $g=[2]_q$ est d'ordre 2^{m+1} dans le groupe $\mathbf{Z}_q^*$. En déduire que si $q \geq 3$ premier divise F_m alors*

$$q \equiv 1 \pmod{2^{m+1}}.$$

Exercice 93 *Soit $l \geq 3$ premier divisant deux nombres de Fermat $F_m = 2^{2^m}+1$ et $F_n = 2^{2^n}+1$. En calculant l'ordre de $g=[2]_l$ dans le groupe $\mathbf{Z}_l^*$, montrer que $m=n$. Autrement dit, deux nombres de Fermat distincts sont premiers entre eux (voir l'Exercice 26 pour une autre solution).*

Exercice 94 *Soit*

$$F_m = 2^{2^m}+1$$

un nombre de Fermat avec $m \geq 2$. Calculer $(2^{3\cdot 2^{m-2}}-2^{2^{m-2}})^2$ modulo F_m, puis montrer que si $q \geq 3$ non nécessairement premier divise F_m alors

$$g := [2^{3\cdot 2^{m-2}}-2^{2^{m-2}}]_q$$

est d'ordre 2^{m+2} dans $\mathbf{Z}_q^*$. Montrer finalement que si $q \geq 3$ premier divise F_m avec $m \geq 2$ alors

$$q \equiv 1 \pmod{2^{m+2}}.$$

Exercice 95 *En considérant le groupe $\mathbf{Z}_p^*$, prouver que $a^{p-1} \equiv 1 \pmod p$ pour tout $a \in \mathbf{Z}$ premier à p, puis montrer que cela implique le petit théorème de Fermat selon lequel $a^p \equiv a \pmod p$ pour tout $a \in \mathbf{Z}$. En déduire que si $p \geq 3$ est premier alors*

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod p.$$

(Voir l'exercice 108 pour l'étude de la réciproque).

Exercice 96 *Preuve de quelques cas particuliers du Théorème de la progression arithmétique (Théorème 30).*

1. *Montrer que si p premier divise un entier de la forme $(2a)^{2^{m-1}}+1$ alors $p \equiv 1 \pmod{2^m}$ (calculer l'ordre de $g = [2a]_p$ dans le groupe $G = \mathbf{Z}_p^*$). En déduire que pour chaque $m \geq 1$ la progression arithmétique $\{2^m k + 1;\ k \geq 0\}$ contient au moins un puis une infinité de nombres premiers (pour en construire un premier p_1, choisir $a = 1$; si $3 \leq p_1 < \cdots < p_n$ sont $n \geq 1$ premiers distincts de cette progression, considérer l'entier $(2p_1p_2\cdots p_n)^{2^{m-1}} + 1$).*

2. *Montrer que si p premier divise $F_{m-1} = 2^{2^{m-1}} + 1$ alors $p \equiv 1 \pmod{2^m}$ (calculer l'ordre de $g = [2]_p$ dans le groupe $G = \mathbf{Z}_p^*$). Montrer de plus par récurence sur m que $F_0F_1\cdots F_{m-1} = F_m - 2$ et en déduire que les F_m, $m \geq 0$, sont deux à deux premiers entre eux. En déduire finalement que pour chaque $m \geq 1$ la progression arithmétique $\{2^m k+1;\ k \geq 0\}$ contient une infinité de nombres premiers (et même que pour tout $x \geq e$ réel il existe au moins $\gg \log\log x$ nombres premiers $p \leq x$ dans la progression arithmétique $\{2^m k + 1;\ k \geq 0\}$).*

3. *Soient $q \geq 2$ premier et $m \geq 1$ fixés.*

   (a) *Montrer que si $p \neq q$ divise un entier N de la forme*

   $$N = 1 + y + y^2 + \cdots + y^{q-1},$$

   alors $g = [y]_p$ est d'ordre q dans le groupe $G = \mathbf{Z}_p^*$, et $p \in \{qk + 1;\ k \geq 0\}$. En déduire que la progression arithmétique $\{qk + 1;\ k \geq 0\}$ contient au moins un puis une infinité de nombres premiers (pour en construire un premier p_1, choisir $y = q$; si $3 \leq p_1 < \cdots < p_n$ sont $n \geq 1$ premiers distincts de cette progression, choisir $y = qp_1p_2\cdots p_n$).

   (b) *En déduire également que si $p \neq q$ divise un entier de la forme*

   $$N = 1 + x^{q^{m-1}} + x^{2q^{m-1}} + \cdots + x^{(q-1)q^{m-1}},$$

   alors $g = [x]_p$ est d'ordre q^m dans le groupe $G = \mathbf{Z}_p^*$ et $p \in \{q^m k + 1;\ k \geq 0\}$, puis que pour chaque $m \geq 1$ la progression arithmétique $\{q^m k + 1;\ k \geq 0\}$ contient au moins un puis une infinité de nombres premiers.

4. *Soit $p \geq 3$ premier fixé.*

   (a) *Soit $a \geq 2$ entier. Montrer que $g = [a]_N$ est d'ordre p dans le groupe $G = \mathbf{Z}_N^*$ où $N := a^p - 1$, et en déduire que p divise $\phi(N) = \phi(a^p - 1)$.*

   (b) *Soient q_i, $1 \leq i \leq k$, des nombres premiers. Montrer que tout diviseur premier l_i de $N = (pq_1\cdots q_r)^p - 1 = l_1^{e_1}\cdots l_s^{e_s}$ est distinct de p et des q_i et qu'au moins un d'entre eux est congru à 1 modulo p.*

   (c) *En déduire que la progression arithmétique $\{kp + 1;\ k \geq 0\}$ contient une infinité de nombre premiers.*

Exercice 97 *Soit G un groupe multiplicatif abélien d'ordre $n \geq 1$ et d'élement neutre 1_G. Pour $x \in G$ on $x^m = 1_G$ si et seulement si $x^{\mathrm{pgcd}(m,n)} = 1_G$.*

Un groupe abélien fini $(G, *)$ d'ordre n est dit **cyclique** si il existe $g \in G$ tel que $G = \{g^k;\ k \in \mathbf{Z}\}$ (où $g^k := g * g * \cdots * g$, g répété k fois pour $k \geq 1$, où $g^0 = 1_G$ et où $g^k = (g^{-k})^{-1}$ pour $k < 0$), donc si et seulement si il existe $g \in G$ d'ordre n dans G. Par exemple, le groupe additif $(\mathbf{Z}_n, +)$ est cyclique d'ordre n engendré par $[1]_n$.

Exercice 98 *Montrer que $[a]_n$ est un générateur du groupe cyclique $(\mathbf{Z}_n, +)$ d'ordre n si et seulement si* $\mathrm{pgcd}(a, n) = 1$.

Théorème 99 *Soit G un groupe multiplicatif cyclique d'ordre $n \geq 1$ et d'élement neutre 1_G. Pour tout entier $m \geq 1$ l'équation $x^m = 1_G$ a* $\mathrm{pgcd}(m, n)$ *solutions dans G. Plus généralement, pour $a \in G$ l'équation $x^m = a$ n'a pas de solution dans G si $a^{n/\mathrm{pgcd}(m,n)} \neq 1_G$ et en a* $\mathrm{pgcd}(m, n)$ *si $a^{n/\mathrm{pgcd}(m,n)} = 1_G$.*

Exercice 100

1. *Montrer que pour $[a]_n \in \mathbf{Z}_n$ on a $k[a]_n = [ka]_n = [0]_n$ si et seulement si $n/$*$\mathrm{pgcd}(a, n)$ *divise k (utiliser le Lemme de Gauss). En déduire que $[a]_n$ est d'ordre $n/$*$\mathrm{pgcd}(a, n)$ *divisant l'ordre n du groupe additif $(\mathbf{Z}_n, +)$.*

2. *Réciproquement, soit $d \geq 1$ divisant n. Montrer $[a]_n$ est d'ordre d dans le groupe additif $(\mathbf{Z}_n, +)$ si et seulement si* $\mathrm{pgcd}(a, n) = n/d$, *et en déduire qu'il y a $\phi(d) := \#\{a;\ 1 \leq a \leq d$ et* $\mathrm{pgcd}(a, d) = 1\}$ *éléments d'ordre d dans le groupe additif $(\mathbf{Z}_n, +)$.*

3. *Pour d divisant n on note E_d l'ensemble des éléments d'ordre d de $(\mathbf{Z}_n, +)$. En remarquant que $\mathbf{Z}_n = \cup_{d|n} E_d$, montrer finalement que $\sum_{d|n} \phi(d) = n$.*

Exercice 101

1. *Soit g un élement d'ordre n dans un groupe multiplicatif $(G, \cdot)$. Montrer que $< g >:= \{g^k;\ k \geq 0\}$ est un sous-groupe d'ordre n de G (qu'on appelle le sous-groupe engendré par g) et montrer que $< g >$ contient $\phi(n)$ élements d'ordre n en montrant que $g^m \in < g >$ est d'ordre n si et seulement si* $\mathrm{pgcd}(m, n) = 1$. *Autrement dit, un groupe cyclique d'ordre n contient $\phi(n)$ éléments d'ordre n.*

2. *Soient p premier, d divisant $p - 1$ et $g \in \mathbf{Z}_p^*$ d'ordre d. Montrer que $< g >= \{x \in \mathbf{Z}_p;\ x^d - 1 = 0\}$ (une inclusion est évidente et utiliser l'Exercice 78 pour en déduire l'égalité). En conséquence, $< g >$ ne dépend donc pas de g mais seulement de d.*

3. *En déduire que si pour un d divsant $p - 1$ le nombre $\psi(d)$ d'éléments d'ordre d de $\mathbf{Z}_p^*$ est non nul, alors $\psi(d) = \phi(d)$, de sorte que dans tous las cas on a $0 \leq \psi(d) \leq \phi(d)$.*

4. *Pour d divisant n on note E_d l'ensemble des éléments d'ordre d de $(\mathbf{Z}_p^*, \cdot)$. En remarquant que $\mathbf{Z}_p^* = \cup_{d|n} E_d$, montrer que $\sum_{d|p-1} \psi(d) = p - 1$, et en remarquant qu'on a également $\sum_{d|p-1} \phi(d) = p - 1$, montrer finalement que $\psi(d) = \phi(d)$ pour tout d divisant $p - 1$.*

5. *Montrer que pour $p \geq 2$ premier le groupe multiplicatif $\mathbf{Z}_p^*$ d'ordre $p - 1$ est cyclique. (Voir le Théorème 105 pour une autre preuve).*

Théorème 102 *Soit G un groupe abélien fini d'ordre $n \geq 1$ et posons*

$$e(G) := \mathrm{ppcm}\{\mathrm{ordre}(g);\ g \in G\}$$

*(on l'appelle l'***exposant du groupe** *abélien fini G). Alors,*

(i) *$e(G)$ divise n.*

(ii) *pour tout $g \in G$ on $g^{e(G)} = 1_G$.*

(iii) *si $m \geq 1$ est tel que pour tout $g \in G$ on a $g^m = 1_G$, alors $e(G)$ divise m. En particulier, on a*

$$e(G) = \min\{k \geq 1;\ g \in G \Rightarrow g^k = 1_G\}.$$

(iv) *il existe un élément de G d'ordre $e(G)$.*

Preuve. Utiliser l'Exercice 88. •

Exercice 103 *Montrer que si G_i, $1 \leq i \leq r$, sont des groupes abéliens finis d'exposants $e(G_i)$, alors le groupe produit $G = \prod_{i=1}^r G_i$ (des r-uplets $(g_1, \cdots, g_r)$ avec $g_i \in G_i$) muni de la loi produit $(g_1, \cdots, g_r)(g'_1, \cdots, g'_r) = (g_1 g'_1, \cdots, g_r g'_r)$) est d'exposant $e(G) = \mathrm{ppcm}(e(G_1), e(G_2), \cdots, e(G_r))$.*

Exercice 104 *Que vaut l'exposant d'un groupe cyclique fini d'ordre $n \geq 1$?*

Théorème 105 *Si $p \geq 3$ est premier, alors le groupe multiplicatif $\mathbf{Z}_p^*$ d'ordre $p-1$ est cyclique.*

Preuve. Soit e_p l'exposant du groupe multiplicatif $\mathbf{Z}_p^*$ d'ordre $p-1$. Alors e_p divise $p-1$, donc $e_p \leq p-1$, et tout $g \in \mathbf{Z}_p^*$ est racine du polynôme $X^{e_p} - 1 \in \mathbf{Z}_p[X]$. D'après l'Exercice 78, on a $p-1 \leq e_p$. D'où $e_p = p-1$. Puisqu'il existe au moins un élément d'ordre $e_p = p-1$ (voir Théorème 102), on a le résultat. (Voir l'exercice 101 pour une autre preuve). •

Exercice 106 *Montrer que si G est cyclique d'ordre n alors g est générateur de G si et seulement si $g^{n/p} \neq 1_G$ pour tout p premier divisant n. En déduire que $g = [2]_{101}$ est générateur de $\mathbf{Z}_{101}^*$ (il faut voir que $g^{50} \neq 1$ et $g^{20} \neq 1$. On calculera donc d'abord $g' = g^{10}$, puis g'^2 et g'^5).*

Exercice 107 *Soit $p \geq 3$ premier et soit $a \in \mathbf{Z}_p^*$. D'après les Théorèmes 99 et 105, l'équation $x^2 = a$ possède au moins une solution $\alpha \in \mathbf{Z}_p^*$ (auquel cas elle en possède deux distinctes, $\pm\alpha$) si et seulement si $a^{(p-1)/2} = 1$. Nous proposons ici une autre preuve de ce résultat n'utilisant pas la cyclicité de $\mathbf{Z}_p^*$.*

1. *Montrer qu'il existe un polynôme unitaire $q(x) \in \mathbf{Z}_p[x]$ de degré $p-3$ tel que*

$$x^{p-1} - 1 = (x^2 - a)q(x) + a^{(p-1)/2} - 1$$

(remarquer que $x^{p-1} - 1 = (x^2)^{(p-1)/2} - 1 = ((x^2 - a) + a)^{(p-1)/2} - 1$).

2. *En déduire que si il existe $\alpha \in \mathbf{Z}_p^*$ tel que $\alpha^2 = a$ alors $a^{(p-1)/2} = 1$.*

3. *Réciproquement, supposons que $a^{(p-1)/2} = 1$. En remarquant qu'alors on a $x^{p-1} - 1 = (x^2 - a)q(x)$ dans $\mathbf{Z}_p[x]$, montrer qu'il existe $\alpha \in \mathbf{Z}_p^*$ tel que $\alpha^2 = a$ (compter les racines dans $\mathbf{Z}_p^*$ de ces polynômes).*

Exercice 108 *Soit $n \geq 3$ entier impair. Posons $S(n) = \sum_{k=1}^n k^{n-1}$.*

1. *Montrer que si n est premier alors $S(n) \equiv -1 \pmod{n}$.*

2. *Réciproquement, soient $n \geq 3$ un entier impair et $p \geq 3$ premier divisant n.*

   (a) *Montrer que*

$$S(n) = \sum_{a=1}^{p} \sum_{b=0}^{(n/p)-1} (a+bp)^{n-1} \equiv \frac{n}{p} \sum_{a=1}^{p-1} a^{n-1} \pmod{p}.$$

   (b) *En utilisant la cyclicité du groupe $\mathbf{Z}_p^*$, montrer que si $p-1$ ne divise pas $n-1$ alors*

$$\sum_{a=1}^{p-1} a^{n-1} \equiv 0 \pmod{p}$$

   et donc $S(n) \not\equiv -1 \pmod{n}$ (fixer $g_0 \in \mathbf{Z}_p^*$ d'ordre $p-1$ dans ce groupe cyclique pour ramener la somme $\sum_{g \in \mathbf{Z}_p^*} g^{n-1}$ à une somme partielle de série géométrique).

   (c) *Montrer que si $p-1$ divise $n-1$ alors*

$$S(n) \equiv \frac{n}{p} \sum_{a=1}^{p-1} a^{n-1} \equiv -\frac{n}{p} \pmod{p}.$$

   En déduire que si de plus $S(n) \equiv -1 \pmod{n}$, alors $n/p \equiv 1 \pmod{p}$.

   (d) *En conclure que $S(n) \equiv -1 \pmod{n}$ si et seulement si tout diviseur premier p de n est tel que $p-1$ divise $n-1$ et $n/p \equiv 1 \pmod{p}$. Montrer qu'un tel n est sans facteur carré (donc est nombre de Carmichael (voir ci-dessous)).*

3. *Soit $n \geq 3$ un entier impair non premier tel que si p premier divise n, alors $n/p \equiv 1 \pmod{p}$. Montrer que n est sans facteur carré et que*

$$N := \sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} = \sum_{p|n} \frac{1}{p} - \frac{1}{n}$$

   est un entier strictement positif (remarquer que $nN = (\sum_{p|n} \frac{n}{p}) - 1$ est clairement entier, puis remarquer qu'il suffit de montrer que $\sum_{p|n} \frac{n}{p} \equiv 1 \pmod{n}$, donc que $\sum_{p|n} \frac{n}{p} \equiv 1 \pmod{p_0}$ pour tout p_0 premier divisant n). En déduire que n possède au moins 9 facteurs premiers (remarquer que si $3 = p_1 < 5 = p_2 < \cdots$ désigne la suite des nombres premiers impairs et si n posède $r \geq 1$ facteurs premiers, alors $\sum_{k=1}^{r} \frac{1}{p_k} \geq \sum_{p|n} \frac{1}{p} > N \geq 1$).

Exercice 109 1. *Soit $p = 8k+1 \equiv 1 \pmod{8}$ premier. En remarquant que $x^{4k}+1 = (x^{2k}+1)^2 - 2(x^k)^2$, montrer que 2 est un carré dans $\mathbf{Z}_p^*$.*

2. *Soit $p = 3k+1 \equiv 1 \pmod{3}$ premier. En remarquant que $4(x^{3k}-1) = 4(x^k-1)(x^{2k}+x^k+1) = (x^k-1)((2x^k+1)^2+3)$, montrer que -3 est un carré dans $\mathbf{Z}_p^*$. En déduire que si $p \equiv 1 \pmod{12}$ est premier alors 3 est un carré dans $\mathbf{Z}_p^*$.*

3. *Réciproquement, supposons que -3 est un carré dans $\mathbf{Z}_p^*$ avec $p > 3$ premier. Montrer qu'il existe $n = 2r+1$ impair tel que $-3 \equiv n^2 \equiv (2r+1)^2 \pmod{p}$, que cela implique $r^2+r+1 \equiv 0 \pmod{p}$, $r^3 \equiv 1 \pmod{p}$ et $r \not\equiv 1 \pmod{p}$, puis implique $p \equiv 1 \pmod{3}$.*

Exercice 110 *Soit $p = 24k+1 \equiv 1 \pmod{24}$. D'après l'Exercice 109, 2 et 3 sont des carrés dans $\mathbf{Z}_p^*$, et donc $2^{(p-1)/2} \equiv 3^{(p-1)/2} \equiv 1 \pmod{p}$. Supposons $p' = (p+1)/2$ premier et posons $n = pp'$ (e.g. $p = 73$, $p' = 37$ et $n = 37 \cdot 73 = 2701$). En remarquant que $(p-1)/2$ divise $n-1$ et que donc $p'-1 = (p-1)/2$ divise $n-1$, montrer que $2^{n-1} \equiv 1 \pmod{p}$ et $2^{n-1} \equiv 1 \pmod{p'}$, donc que $2^{n-1} \equiv 1 \pmod{n}$, et que $3^{n-1} \equiv 1 \pmod{p}$ et $3^{n-1} \equiv 1 \pmod{p'}$, et donc que $3^{n-1} \equiv 1 \pmod{n}$, c'est à dire que n est 2-pseudopremier et 3-pseudopremier.*

4.2 Certificats de primalité

Exercice 111 *Montrer que si $n > 1$ est premier alors il existe a tel que $a^{(n-1)/2} \equiv -1 \pmod{n}$ (la réciproque est-elle vraie?). Montrer que si un nombre de Fermat $n = 2^{2^m} + 1$ est tel qu'il existe $a \geq 1$ tel que $a^{(n-1)/2} \equiv -1 \pmod{n}$ alors n est premier (montrer que 2 est d'ordre $n-1$ dans $\mathbf{Z}_n^*$). En déduire que $F_m = 2^{2^m} + 1$ est premier si et seulement si il existe a tel que $a^{(F_m-1)/2} \equiv -1 \pmod{F_m}$. Les nombres de Fermat ont donc des certificats de primalité polynomiaux.*

3 est certificat de primalité pour $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$:

k	$3^{2^k} \pmod{F_1}$	$3^{2^k} \pmod{F_2}$	$3^{2^k} \pmod{F_3}$	$3^{2^k} \pmod{F_4}$
0	3	3	3	3
1	$4 = -1$	9	9	9
2		13	81	81
3		$16 = -1$	136	6561
4			249	54449
5			64	61869
6			241	19139
7			$256 = -1$	15028
8				282
9				13987
10				8224
11				65529
12				64
13				4096
14				65281
15				$65536 = -1$

Théorème 112 *(Test de primalité polynomial des nombres de Fermat). Pour $m \geq 1$ le nombre de Fermat $F_m = 2^{2^m} + 1$ est premier si et seulement si $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$.*

Preuve. Si $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$ alors F_m est premier d'après l'Exercice 111. Réciproquement, supposons $F_m = p$ premier. Puisque $p \equiv (-1)^{2^m} + 1 \equiv 2 \pmod{3}$, alors d'après l'Exercice 109, -3 n'est pas un carré dans $\mathbf{Z}_p^*$. Nous avons donc $3^{(p-1)/2} = (-3)^{(p-1)/2} \not\equiv 1 \pmod{p}$ (car $p \equiv 1 \pmod{4}$), et donc $3^{(p-1)/2} \equiv -1 \pmod{p}$. •

Exercice 113 *Montrer que si m divise n alors $2^m - 1$ divise $2^n - 1$. En déduire que si $2^{n-1} \equiv 1 \pmod{n}$ alors $2^{m-1} \equiv 1 \pmod{m}$ où $m = 2^n - 1$. Montrer finalement qu'il existe une infinité d'entiers impairs non premiers N tels que $2^{N-1} \equiv 1 \pmod{N}$*

Théorème 114 *Pour $a > 1$ entier fixé, il existe une infinité d'entiers impairs non premiers n tels que $a^{n-1} \equiv 1 \pmod{n}$.*

Preuve. Nous la laissons en exercice : soient $p \geq 2$ premier ne divisant pas $a(a^2-1)$ (ce qui implique $p > 3$) et $n = (a^{2p}-1)/(a^2-1) = 1 + a^2 + \cdots + a^{2(p-1)}$ (et $n > 1$ est donc impair).

1. Montrer que n n'est jamais premier.
2. Montrer que $a^2 \not\equiv 1 \pmod{n}$ (minorer n en fonction de a^2) et que $a^{2p} \equiv 1 \pmod{n}$. En déduire que a^2 est d'ordre p dans $\mathbf{Z}_n^*$ et que a est d'ordre p ou $2p$ dans $\mathbf{Z}_n^*$.
3. Montrer que p divise $n-1$ (remarquer que $n - 1 = a^2(a^{2(p-1)} - 1)/(a^2 - 1)$), puis que $2p$ divise $n - 1$.

4. En déduire que $a^{n-1} \equiv 1 \pmod{n}$.

5. En déduire que pour $a > 1$ fixé il existe une infinité d'entiers impairs non premiers n tels que $a^{n-1} \equiv 1 \pmod{n}$. •

Définition 115 *Soit $n \geq 3$ impair. Écrivons $n-1 = 2^m n'$ avec n' impair. On dit que a est un* **témoin de composition** *de n si il vérifie*
(i) $\mathrm{pgcd}(a, n) = 1$,
(ii) $a^{n'} \not\equiv 1 \pmod{n}$,
et (iii) $a^{2^k n'} \not\equiv -1 \pmod{n}$ *pour* $0 \leq k \leq m-1$.

Exercice 116 *Montrer que pour $p > 3$ premier le rationnel $n = (4^p + 1)/5$ est un entier non premier (développer $(x^p + x^{(p+1)/2} + 1)(x^p - x^{(p+1)/2} + 1)$) mais que $a = 2$ n'est jamais témoin de composition de n (commencer par remarquer que $n - 1 \equiv 4 \pmod{8}$, qui donne $n - 1 = 2^2 n'$ avec n' impair, et montrer que $2^{2n'} \equiv -1 \pmod{n}$).*

Théorème 117 *Soit $n \geq 3$ un entier impair. Alors, n est composé si et seulement si il admet au moins un témoin de composition.*

Preuve. Nous ne prouvons qu'un sens (le second sera prouvé à l'exercice 142): supposons n premier et montrons qu'il n'admet pas de témoin de composition. Soit en effet a vérifiant (i) et (ii). Puisque $a^{2^m n'} = a^{n-1} \equiv 1 \pmod{n}$ (par (i) et le théorème de Fermat) mais $a^{2^0 n'} = a^{n'} \not\equiv 1 \pmod{n}$ (par (ii)), alors $k_0 := \max\{k \geq 0;\ a^{2^k n'} \not\equiv 1 \pmod{n}\}$ est bien défini, $k_0 \in \{0, \cdots, m-1\}$ et $b := a^{2^{k_0} n'}$ vérifie $b \not\equiv 1 \pmod{n}$ et $b^2 \equiv 1 \pmod{n}$. D'où $b \equiv -1 \pmod{n}$ (car n est supposé premier) et (iii) n'est pas vérifié. •

Exercice 118 *Montrer que $n > 1$ est premier si et seulement si il existe $a \in \mathbf{Z}$ tel que $a^{n-1} \equiv 1 \pmod{n}$ mais $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ pour tout diviseur premier q de n (déterminer d'abord pour un tel a l'ordre de $[a]_n$ dans le groupe multiplicatif $\mathbf{Z}_n^*$).*

Théorème 119 *(Pratt (1975)). Tout premier $n \geq 3$ admet un certificat de primalité polynomial.*

Preuve. Écrivons
(i) $n - 1 = \prod_{i=1}^{k} q_i$
avec
(ii) les q_i premiers.
D'après l'exercice précédent, n est premier si et seulement si il existe a tel que
(iii) $a^{n-1} \equiv 1 \pmod{n}$ et $a^{(n-1)/q_i} \not\equiv 1 \pmod{n}$ pour tout $1 \leq i \leq k$.
Pour certifier que n est premier, on donne a, les q_i et on demande de vérifier (i) et (iii), et on vérifie (ii) récursivement. •

Exemple 120 *On a $F_{10} := 2^{2^{10}} + 1 = 2^{1024} + 1 = 4559257 \cdot 6487031809 \times n_{291}$ où n_{291} est un nombre de 291 chiffres qu'on sait être composé (car il vérifie $2^{n_{291}-1} \not\equiv 1 \pmod{n}$), mais dont on ne connait pas la factorisation. Justifions que le facteur $n_{10} = 6487031809$ est premier. On vérifie que $n_{10} - 1 = 2^{14} \cdot 3^2 \cdot 29 \cdot 37 \cdot 41$, que 2, 3, 29, 37 et 41 sont premiers et que (iii) est satisfaite avec $a = 7$.*

4.3 Cryptographie à clé révélée

Exercice 121 *Soient $n > 1$ impair et $m \equiv 1 \pmod{\phi(n)}$. Expliquer pourquoi $w^m \equiv w \pmod{n}$ pour tout w premier à n. Montrer de plus que si n est sans facteur carré, alors $w^m \equiv w \pmod{n}$ pour tout w (soient $n_1 := \mathrm{pgcd}(w, n) > 1$ et $n_2 = n/n_1$. Remarquer que $\mathrm{pgcd}(n_1, n_2) = 1$, que $n_1 n_2 = n$, que $w^m \equiv w \pmod{n_1}$ et que $w^m \equiv w \pmod{n_2}$).*

Le système RSA (Rivest, Shamir et Adleman (1978)). Soit $n = pq$ (*module d'encodage*) produit de deux nombres premiers impairs p et q distincts. Soit $e > 1$ (*exposant d'encodage*) premier à $\phi(n) = (p-1)(q-1)$ et soit d tel que $ed \equiv 1 \pmod{\phi(n)}$. Les deux entiers n et e sont publics, mais la factorisation $n = pq$ du module d'encodage n est gardée secrète ce qui rend le calcul de $\phi(n)$ et donc de e probablement difficiles (voir Lemme ci-dessous). Soit w (écrit dans l'alphabet $\{0, \cdots, 9\}$) un texte à coder avec $0 \leq w < n$. Soit $w' = w^e$ modulo n (*texte crypté*). Alors, $w'^d = w^{de} \equiv w \pmod{n}$. Donc la connaissance de d permet de retrouver w.

Lemme 122 *Si on connait n et $\phi(n)$ alors on connait la factorisation $n = pq$ de n.*

Preuve. $\phi(n) = (p-1)(q-1) = n - (p+q) + 1$ et $(p-q)^2 = (p+q)^2 - 4pq$ donnent $p + q = n + 1 - \phi(n)$ et $p - q = \sqrt{(n+1-\phi(n))^2 - 4n}$. •

Exercice 123 *Montrons que A doit être prudent dans le choix de son exposant d'encodage public e. Supposons que B utilise les données publiques e et n de A pour coder son message w. Il envoie donc $w' = f(w) := w^e \pmod{n}$ par une voix non protégée. Un tiers C intercepte ce message codé w' et utilise les données publiques e et n de A pour coder répétitivement ce message crypté w' en calculant $f^2(m) := f(fm)) = f(w')$, $f^3(m) := f(f^2(m)), \cdots$. Montrer que si e est d'ordre k dans $\mathbf{Z}^*_{\phi(n)}$ alors $f^{k-1}(w') = w$, c'est à dire que si la clé d'encodage e est mal choisie alors tout tiers C peut aisément décrypter tout message crypté avec les clés publiques de A.*

5 Structure de $\mathbf{Z}^*_n$

5.1 Structure de $\mathbf{Z}^*_{p^n}$

Exercice 124

1. *Montrer que pour tout $k \geq 0$ entier on a $2^{3^k} \equiv 3^{k+1} - 1 \pmod{3^{k+2}}$. En déduire que $g_n := [2]_{3^n}$ est d'ordre $2 \cdot 3^{n-1}$ dans $\mathbf{Z}^*_{3^n}$ puis que ce groupe multiplicatif $\mathbf{Z}^*_{3^n}$ est cyclique engendré par g_n.*
2. *Montrer que pour tout $k \geq 0$ entier on a $2^{2 \cdot 5^k} \equiv 5^{k+1} - 1 \pmod{5^{k+2}}$. En déduire que $h_n := [2]_{5^n}$ est d'ordre $4 \cdot 5^{n-1}$ dans $\mathbf{Z}^*_{5^n}$ puis que ce groupe multiplicatif $\mathbf{Z}^*_{5^n}$ est cyclique engendré par h_n.*

Théorème 125 *Si $p \geq 3$ est premier et $n \geq 1$ est entier, alors le groupe multiplicatif $\mathbf{Z}^*_{p^n}$ est cyclique d'ordre $(p-1)p^{n-1}$. Plus précisément, si $g_p \in \mathbf{Z}$ est tel que sa classe modulo p engendre $\mathbf{Z}^*_p$, alors $G_p = g_p$ ou $G_p = g_p + p$ vérifie $G_p^{p-1} \not\equiv 1 \pmod{p^2}$, et pour tout $n \geq 1$ la classe modulo p^n de G_p engendre le groupe multiplicatif $\mathbf{Z}^*_{p^n}$. En conséquence, l'équation $x^2 = 1$ n'a que deux solutions dans $\mathbf{Z}^*_{p^n}$, à savoir $x = 1 := [1]_{p^n}$ et $x = -1 := [-1]_{p^n}$.*

Preuve. Écrivons $H_p := G_p^{p-1} = 1 + \lambda p$. On commence par montrer par récurrence sur $k \geq 0$ que $H_p^{p^k} \equiv 1 + \lambda p^{k+1} \pmod{p^{k+2}}$. On en déduit que la classe de H_p est d'ordre p^{n-1} dans $\mathbf{Z}^*_{p^n}$,

puis que la classe de G_p est donc d'ordre $d \cdot p^{k-1}$ divisant $(p-1) \cdot p^{k-1}$ dans $\mathbf{Z}_{p^n}^*$. On remarque ensuite que $G_p^{dp^{k-1}} \equiv 1 \pmod{p^n}$ implique $1 \equiv G_p^{dp^{k-1}} \equiv g_p^{dp^{k-1}} \equiv g_p^d \pmod{p}$ (pour cette dernière congruence, remarquer que $p-1$ divise $p^{k-1}-1$), donc que l'ordre $p-1$ de g_p dans $\mathbf{Z}_p^*$ divise d, donc que $d = p-1$. La classe modulo p^n de G_p est donc d'ordre $(p-1) \cdot p^{n-1} = \phi(p^n)$ dans le groupe $\mathbf{Z}_{p^n}$ d'ordre $\phi(p^n)$, ce qui prouve les résultats annoncés. •

Exercice 126 *Utiliser le théorème chinois des restes et le théorème précédent pour montrer que si $n > 1$ impair possède t diviseurs premiers impairs distincts, alors l'équation $x^2 = 1$ posssède 2^t solutions dans $\mathbf{Z}_n$.*

Exercice 127 *Nous montrons que si $n \geq 3$ impair est tel que $a^{n-1} \equiv 1 \pmod{n}$ pour tout a premier à n, alors est sans facteur carré. Soient p premier divisant n et $e = v_p(n)$. Il s'agit de voir que $e = 1$. Soit $g \in \mathbf{Z}$ un générateur du groupe cyclique $\mathbf{Z}_{p^e}^*$. Expliquer pourquoi $g^{n-1} = 1$, puis montrer que $\phi(p^e)$ divise $n-1$, puis que $e = 1$.*

Exercice 128

1. *Rappeler la formule donnant le nombre de solutions $x \in G$ de l'équation $x^m = 1_G$ dans un groupe multiplicatif cyclique fini G d'ordre n et de neutre 1_G.*
2. *Soit p^k une puissance d'un premier $p \geq 3$ et $N \geq 1$ divisible par p^k.*
   (a) *Montrer que l'équation $x^N = x$ a $\mathrm{pgcd}(N-1, p-1)$ solutions $x \in \mathbf{Z}_{p^k}^*$.*
   (b) *Montrer que si p divise X où $x = [X]_{p^k}$ alors p^k divise X^N. En déduire que l'équation $x^N = x$ a $1 + \mathrm{pgcd}(N-1, p-1)$ solutions $x \in \mathbf{Z}_{p^k}$.*

5.2 Structure de $\mathbf{Z}_{2^n}^*$

Exercice 129 *Soit $a \in \mathbf{Z}$ impair. Montrer par récurrence sur $n \geq 3$ que $a^{2^{n-2}} \equiv 1 \pmod{2^n}$. Qu'en déduit-on pour l'exposant du groupe multiplicatif $\mathbf{Z}_{2^n}^*$? Ce groupe est-il cyclique?*

Théorème 130 *Pour $n \geq 3$ la classe de 5 modulo 2^n est d'ordre 2^{n-2}, celle de -1 est d'ordre 2 et $\mathbf{Z}_{2^n}^* = \{\pm 5^k; 0 \leq k < 2^{n-2}\}$.*

Exercice 131

1. *Combien le polynôme $P(X) = X^2 - 1 \in \mathbf{Z}_8[X]$ a t-il de racines dans $\mathbf{Z}_8$?*
2. *Montrer que pour $p \geq 3$ premier le polynôme $X^2 - 1$ n'a que deux racines dans $\mathbf{Z}_{p^r}^*$: 1 et -1.*

5.3 Structure de $\mathbf{Z}_n^*$

Exercice 132 *Soit $1 < n = \prod_{p|n} p^{e_p}$. Posons*

$$\Lambda(n) := \mathrm{ppcm}_{p|n}(\phi(p^{e_p})) = \phi(n)/\mathrm{pgcd}_{p|n}(\phi(p^{e_p}))$$

(d'après le Théorème 75 et l'Exercice 45), et remarquons que $\Lambda(n)$ divise $\phi(n)$.

1. *Montrer que tout $g = [x]_n \in \mathbf{Z}_n^*$ vérifie $g^{\Lambda(n)} = 1$ (remarquer que d'après l'Exercice 42 il suffit de montrer que tout $g \in \mathbf{Z}_{p^{e_p}}^*$ vérifie $g^{\Lambda(n)} = 1$).*
2. *Montrer que $\phi(p^e) = (p-1)p^{e-1}$.*

3. *Montrer que si n est impair et possède au moins deux facteurs premiers distincts, ou que si n est divisible par 4 et possède au moins deux facteurs premiers distincts, alors $\Lambda(n)$ divise $\phi(n)/2$ et le groupe multiplicatif $\mathbf{Z}_n^*$ ne contient pas d'élément d'ordre $\phi(n)$, i.e. n'est pas cyclique.*

Théorème 133 *Pour $n \geq 2$ entier le groupe multiplicatif $\mathbf{Z}_n^*$ est cyclique si et seulement si $n = 1$, $n = 2$, $n = 4$, $n = p^k$ avec $p \geq 3$, ou $n = 2p^k$ avec $p \geq 3$.*

6 Nombres de Carmichael

Théorème 134 *Soit $n > 2$ entier. Les assertions suivantes sont équivalentes :*

1. *Pour tout entier a premier à n on a $a^{n-1} \equiv 1 \pmod{n}$.*
2. *n est impair, sans facteur carré et tel que $p-1$ divise $n-1$ pour tout facteur premier p de n.*
3. *Pour tout entier a on a $a^n \equiv a \pmod{n}$.*

Un tel entier impair $n > 2$ est appelé un **nombre de Carmichael**.

Preuve. (Voir également l'exercice 140). Supposons la première propriété vraie et montrons que la seconde l'est. Cela résulte de ce que l'exposant e_n du groupe $\mathbf{Z}_n^*$ doit diviser $n-1$, de ce que cet exposant est toujours pair pour $n > 2$, ce qui donne l'imparité de n, et de ce que pour n impair on a $e_n = \mathrm{ppcm}(p-1,\ p \mid n) \times \prod_{p|n} p^{v_p(n)-1}$. Supposons maintenant la seconde propriété vraie et montrons que la troisième l'est. Tout d'abord, il suffit de voir que pour tout p premier divisant n on a $a^n \equiv a \pmod{p}$. Si a est premier à p cela résulte de ce que $p-1$ divisant $n-1$ on a $a^{n-1} \equiv 1 \pmod{p}$; si p divise a cela est encore vrai. Finalement, si la troisième propriété est vraie alors la première l'est aussi. •

Exercice 135 (i). *Vérifier que* 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841 *et* 29341 *sont des nombres de Carmichael.* (i). *Montrer que tout nombre de Carmichael $n > 2$ qui n'est pas premier posssède au moins trois facteurs premiers.* (iii). *Montrer que si pour un entier $k \geq 1$ les trois nombres $6k+1$, $12k+1$ et $18k+1$ sont simultanément premiers, alors leur produit $n = (6k+1)(12k+1)(18k+1)$ est un nombre de Carmichael. Donner les trois plus petites valeurs de $k \geq 1$ pour lesquelle cela se produit.*

Théorème 136 *(Alford, Granville et Pomerance (1994)). Pour $x > 1$ suffisamment grand il y a au moins $x^{2/7}$ nombres de Carmichael inférieurs ou égaux à x.*

7 Tests de primalité probabilistes

Exercice 137 *Soit $n > 1$ de factorisation*

$$n = \prod_{p|n} p^{e_p}.$$

Pour $a = [A]_n \in \mathbf{Z}_n$ on pose $a_{p^{e_p}} = [A]_{p^{e_p}}$. Utiliser le Théorème chinois des restes pour montrer que pour $a \in \mathbf{Z}_n$ (respectivement pour $a \in \mathbf{Z}_n^*$) le nombre $N(n,d,a)$ (respectivement $N^*(n,d,a)$) de solutions dans $\mathbf{Z}_n$ (respectivement dans $\mathbf{Z}_n^*$) de l'équation $x^d = a$ vaut $\prod_{p|n} N(p^{e_p}, d, a_{p^{e_p}})$ (respectivement $\prod_{p|n} N^*(p^{e_p}, d, a_{p^{e_p}})$).

Soit $n > 1$ impair. Écrivons $n - 1 = 2^r m$ avec $r \geq 1$ et $m \geq 1$ impair. Nous posons
$G_0(n) = \mathbf{Z}_n^*$,
$G_1(n) = \{a \in G_0;\ a^{n-1} = 1\}$,
et $G_2(n) = \{a \in G_0,\ a^m = 1 \text{ ou } \exists i \in \{0, 1, \cdots, r-1\} / a^{2^i m} = -1\}$.

Exercice 138 *Posons $F_n = 2^{2^n} + 1$. Déterminer l'ordre de 2 dans $G_0(F_n) = \mathbf{Z}_{F_n}^*$. En déduire que pour tout $n \geq 0$ on a $2 \in G_1(F_n)$. Montrer également que $2 \in G_2(F_n)$.*

Exercice 139 *Montrer que $G_2(n) \subseteq G_1(n) \subseteq G_0(n)$, que $G_1(n)$ est un sous-groupe de $G_0(n)$, et donner des exemples de valeurs de n pour lesquelles $G_2(n)$ n'est pas un sous-groupe de $G_0(n)$.*

Exercice 140

1. *Montrer que si G est un groupe cyclique d'ordre n alors pour tout $d \geq 1$ le nombre de solutions $g \in G$ de l'équation $g^d = 1_G$ vaut* $\mathrm{pgcd}(d, n)$.

2. *En déduire (en utilisant le théorème chinois des restes) que pour $n \geq 3$ impair $G_1(n)$ est un sous-groupe d'ordre*
$$\#G_1(n) = \prod_{p|n} \mathrm{pgcd}(p-1, n-1).$$

3. *Montrer finalement que pour $n \geq 3$ impair on a $G_1(n) = G_0(n)$ si et seulement si n est sans facteur carré et tel que p divise n implique $p-1$ divise $n-1$. Donner des exemples de valeurs de $n \geq 3$ impairs non premiers pour lesquelles $G_1(n) = G_0(n)$ (Comparer ces résultats avec ceux du Théorème 134).*

Exercice 141

1. *Montrer que si G est un groupe cyclique d'ordre n alors pour tout $d \geq 1$ le nombre de solutions $g \in G$ de l'équation $g^d = 1_G$ vaut* $\mathrm{pgcd}(d, n)$.

2. *En déduire (en utilisant le théorème chinois des restes) que pour $n \geq 3$ impair on a*
$$\#\{a \in \mathbf{Z}_n;\ a^n = a\} = \prod_{p|n} (1 + \mathrm{pgcd}(p-1, n-1)).$$

3. *Montrer finalement que pour $n \geq 3$ impair on a $\{a \in \mathbf{Z}_n;\ a^n = a\} = \mathbf{Z}_n$ si et seulement si n est sans facteur carré et tel que p divise n implique $p-1$ divise $n-1$. Donner des exemples de valeurs de $n \geq 3$ impairs non premiers pour lesquelles $\{a \in \mathbf{Z}_n;\ a^n = a\} = \mathbf{Z}_n$ (Comparer ces résultats avec ceux du Théorème 134).*

Exercice 142 *Soit $n > 1$ impair. Écrivons $n-1 = 2^r m$ avec $m \geq 1$ impair et $r \geq 1$. Nous notons $\omega(n)$ le nombre de diviseurs premiers distincts de n, et pour chacun des $\omega(n)$ diviseurs premiers p de n nous écrivons $p-1 = 2^{r_p} m_p$ avec $m_p \geq 1$ impair et $r_p \geq 1$, et nous posons finalement $\nu(n) := \min_{p|n} r_p \geq 1$.*

1. *Montrer que pour $d \geq 1$ le nombre de solutions de $x^d = 1$ dans $\mathbf{Z}_{p^e}^*$ vaut $\mathrm{pgcd}(d, \phi(p^e))$.*
2. *Montrer que $y \in \mathbf{Z}_{p^e}^*$ vérifie y^2 si et seulement si $y \in \{\pm 1\}$, et en déduire que pour $d \geq 1$ le nombre de solutions de $x^d = -1$ dans $\mathbf{Z}_{p^e}^*$ vaut $\mathrm{pgcd}(2d, \phi(p^e)) - \mathrm{pgcd}(d, \phi(p^e))$.*
3. *Montrer que pour tout $p \geq 3$ premier impair divisant n et tout $k \geq 0$ on a*
$$\mathrm{pgcd}(2^k m, \phi(p^e)) = 2^{\min(k, r_p)} \times \mathrm{pgcd}(m, p-1).$$
4. *Montrer que pour $k \geq 0$ le sous groupe $H_k := \{a \in \mathbf{Z}_n^*;\ a^{2^k m} = 1\}$ de $\mathbf{Z}_n^*$ est d'ordre*
$$\prod_{p|n} 2^{\min(k, r_p)} \times \mathrm{pgcd}(m, p-1)$$
et que le sous-ensemble $H'_k := \{a \in \mathbf{Z}_n^*;\ a^{2^k m} = -1\}$ de $\mathbf{Z}_n^*$ est de cardinal
$$\prod_{p|n} (2^{\min(k+1, r_p)} - 2^{\min(k, r_p)}) \times \mathrm{pgcd}(m, p-1)$$
$$= \begin{cases} 0 & \text{si } k \geq \nu(n) \\ 2^{k\omega(n)} \prod_{p|n} \mathrm{pgcd}(m, p-1) & \text{si } 0 \leq k \leq \nu(n)-1 \end{cases}.$$
5. *Montrer que $\nu(n) \leq r$.*
6. *Montrer que $G_2(n)$ est d'ordre*
$$\#G_2(n) = \Big(1 + \frac{2^{\nu(n)\omega(n)} - 1}{2^{\omega(n)} - 1}\Big) \prod_{p|n} \mathrm{pgcd}(m, p-1).$$
7. *En remarquant que*
$$\begin{aligned} \#G_2(n) &\leq 2^{\nu(n)\omega(n)} \prod_{p|n} \mathrm{pgcd}(m, p-1) \\ &= \prod_{p|n} \mathrm{pgcd}(2^{\nu(n)} m, p-1) \\ &\leq \prod_{p|n} \mathrm{pgcd}(n-1, p-1) \\ &\leq \prod_{p|n} (p-1) \\ &\leq \phi(n) \end{aligned}$$
et que cette première inégalité n'est une égalité que pour $\omega(n) = 1$, c'est à dire lorsque n est puissance d'un nombre premier, alors que cette dernière inégalité n'est une égalité que pour n sans facteur carré, montrer que $G_2(n) = G_0(n)$ si et seulement si n est premier.

8 Sujets d'examen

Faculté des Sciences de Luminy
Année 2001/2002

DEUG 2 MIAS + MASS MF & SE
Option : Arithmétique. Examen de Juin 2002
Aucun document autorisé. Calculatrice autorisée. Durée : 3 heures

Exercice 1. Utiliser l'algorithme d'Euclide pour calculer $d := \mathrm{pgcd}(73, 59)$. "Remonter" alors cet algorithme pour trouver u et v entiers relatifs tels que $u \cdot 73 - v \cdot 59 = d$ (Bézout). En déduire $[59]_{73}^{-1}$ dans $\mathbf{Z}_{73}^*$.

Exercice 2. Soit $(F_n)_{n\geq 0}$ la suite définie par récurrence par $F_0 = F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour $n \geq 0$. Soit $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Montrer que

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = A^n \begin{pmatrix} F_1 \\ F_0 \end{pmatrix}.$$

Expliquer alors un algorithme efficace de calcul de F_n modulo m, l'appliquer au calcul de F_{64} modulo 11 (disposer les calculs matriciels requis de manière à limiter le nombre de matrices à écrire), et montrer que ces calculs montrent que l'ordre de $A \in GL_2(\mathbf{Z}_{11})$ (=les matrices carrées 2×2 à coefficients dans $\mathbf{Z}_{11}$ admettant un inverse à coefficients dans $\mathbf{Z}_{11}$) est d'ordre divisant 10 dans le groupe multiplicatif $(GL_2(\mathbf{Z}_{11}), \cdot)$.

Exercice 3. Soit $p \geq 2$ un nombre premier.
1. Redonner la preuve vue en TD de ce que si $q \geq 2$ premier divise un nombre de Mersenne $M_p := 2^p - 1$ avec $p \geq 2$ premier, alors $q \equiv 1 \pmod{p}$. Application : montrer que $M_{11} = 2047$ n'est pas premier en en donnant un diviseur premier.
2. Montrer que si $a > b \geq 1$ et $m \geq 2$ sont entiers et si $N = a^m - b^m$ est premier, alors (i) $\mathrm{pgcd}(a, b) = 1$, (ii) $a = b + 1$ et (iii) m est premier.
3. Soient $a > b \geq 1$ entiers premiers entre eux et $p \geq 2$ premier. Soit $q \geq 2$ premier divisant $a^p - b^p$. Montrer que q ne divise ni a ni b, et montrer et que si q ne divise pas $a - b$ alors $q \equiv 1 \pmod{p}$. Application : montrer que $N = 3^{11} - 2^{11} = 175099$ n'est pas premier en en donnant un diviseur premier.

Exercice 4. Soit $p \geq 2$ premier et $M_p := 2^p - 1$. Expliquer pourquoi p divise $2^{p-1} - 1$ et, en écrivant $2^{p-1} - 1 = kp$, montrer que $2^{(M_p-1)/2} \equiv 1 \pmod{M_p}$.

Exercice 5. Soient $p \geq 3$ premier et $a \in \mathbf{Z}$ premier à p. On suppose que l'équation $x^2 \equiv a \pmod{p}$ admet une solution $x_1 \in \mathbf{Z}$. Le but de cet exercice est de développer un algorithme efficace de calcul par récurrence sur $m \geq 1$ de solutions $x_m \in \mathbf{Z}$ aux équations

$$x^n \equiv a \pmod{p^m} \quad (m \geq 1).$$

On suppose donc x_m construite et on cherche x_{m+1} sous la forme

$$x_{m+1} = x_m - kp^m \quad (k \in \mathbf{Z}).$$

Montrer qu'un tel x_{m+1} est solution de l'équation $x_{m+1}^2 \equiv a \pmod{p^{m+1}}$ si et seulement si k vérifie

$$2kx_m \equiv (x_m^2 - a)/p^m \pmod{p}.$$

Expliquer pourquoi il existe toujours un tel $k \in \mathbf{Z}$ et expliquer comment on peut numériquement le calculer efficacement. Application : sachant que $x_1 = 4$ est solution de $x^2 \equiv 5 \pmod{11}$,

utiliser cet algorithme pour construire des solutions aux équations $x^2 \equiv 5 \pmod{11^m}$ pour $1 \leq m \leq 3$ (les vérifier une fois trouvées !).

Exercice 6. Soient $p \geq 3$ premier et $a \in \mathbf{Z}_p^*$.
1. Montrer que $x = [1]_p$ et $x = [-1]_p$ sont les seules solutions $x \in \mathbf{Z}_p$ de l'équation $x^2 = [1]_p$, et montrer qu'elles sont distinctes.
2. Montrer que si l'équation $x^2 = a$ a au moins une solution $x \in \mathbf{Z}_p$ alors $a^{(p-1)/2} = 1$. Utiliser ensuite la cyclicité du groupe multiplicatif $\mathbf{Z}_p^*$ pour montrer réciproquement que si $a^{(p-1)/2} = 1$ alors l'équation $x^2 = a$ a au moins une solution dans $\mathbf{Z}_p$ (si g est un générateur de $\mathbf{Z}_p^*$ et $a = g^m$, montrer d'abord que m est pair).
3. Supposons de plus que $p \equiv 3 \pmod 4$ et soit $a \in \mathbf{Z}_p^*$ tel que $a^{(p-1)/2} = 1$. Montrer que les solutions $x \in \mathbf{Z}_p$ de l'équation $x^2 = a$ sont $x = \pm a^{(p+1)/4}$. On choisit $p = 103$ et $a = [2]_{103}$ et on pose $x_k = a^{2^k}$. Calculer x_0, x_1, x_2, x_3, x_4 et x_5 (présenter le résultat sous forme de tableau), puis $a^{(p-1)/2} = a^{51}$ et $b := a^{(p+1)/4} = a^{26}$, et vérifier que $b^2 = 2$.

Faculté des Sciences de Luminy
Année 2001/2002

DEUG 2 MIAS + MASS MF & SE
Option : Arithmétique. Examen de Septembre 2002
Aucun document autorisé. Calculatrice autorisée. Durée : 3 heures

Exercice 1. Utiliser l'algorithme d'Euclide pour calculer $d := \mathrm{pgcd}(132, 73)$ et trouver u et v entiers relatifs tels que $u \cdot 132 - v \cdot 73 = d$ (Bézout).
En déduire $[73]_{132}^{-1}$ dans $\mathbf{Z}_{132}^*$.

Exercice 2. Donner l'ordre de $g = [2]_{17}$ dans le groupe multiplicatif $\mathbf{Z}_{17}^*$. En déduire sans calcul l'ordre de $g' = [4]_{17}$ dans ce même groupe multiplicatif $\mathbf{Z}_{17}^*$. Donner l'ordre du groupe multiplicatif $\mathbf{Z}_{315}^*$.

Exercice 3. Soit $(F_n)_{n\geq 0}$ la suite d'entiers définie par récurrence par $F_1 = F_0 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour $n \geq 0$. On définit alors les matrices colonnes V_n par

$$V_n := \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} \quad (n \geq 0).$$

1. Soit $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Montrer par récurrence sur $n \geq 0$ que

$$V_n = A^n V_0.$$

2. Soit $A_k := A^{2^k}$, $k \geq 0$. Que vaut A_0? Exprimer A_{k+1} à partir de A_k.
3. Calculer alors A^{64} modulo 11 (disposer les calculs matriciels requis de manière à limiter le nombre de matrices à écrire).
4. En déduire V_{64} modulo 11, puis F_{64} modulo 11.

Exercice 4. Soit $p \geq 2$ un nombre premier.
1. Redonner la preuve vue en TD de ce que si $q \geq 2$ premier divise un nombre de Mersenne $M_p := 2^p - 1$ avec $p \geq 2$ premier, alors $g = [2]_q$ est d'ordre p dans le groupe multiplicatif $G := \mathbf{Z}_q^*$ et de ce que cela implique $q \equiv 1 \pmod p$. Application : montrer que $M_{11} = 2047$ n'est pas premier en en donnant un diviseur premier.
2. Soient $a > b \geq 1$ entiers premiers entre eux et $p \geq 2$ premier. Soit $q \geq 2$ premier divisant $a^p - b^p$. Montrer que q ne divise ni a ni b. Montrer que si q ne divise pas $a - b$, alors $g = [a]_q[b]_q^{-1}$ est bien défini et est d'ordre p dans le groupe multiplicatif $G := \mathbf{Z}_q^*$ et que cela implique $q \equiv 1$

(mod p). Application : montrer que $N = 3^{11} - 2^{11} = 175099$ n'est pas premier en en donnant un diviseur premier.

Exercice 5. Soient $p \geq 3$ premier et $a \in \mathbf{Z}_p^*$.
1. Montrer que si $x = [X]_p \in \mathbf{Z}_p$ est solution de l'équation $x^2 = [1]_p$, alors p divise $(X-1)(X+1)$ et montrer que cela implique $x = [1]_p$ ou $x = [-1]_p$.
2. Expliquer pourquoi tout $x \in \mathbf{Z}_p^*$ vérifie $x^{p-1} = [1]_p$.
3. Montrer que si l'équation $x^2 = a$ a au moins une solution $x \in \mathbf{Z}_p$, alors $a^{(p-1)/2} = 1$.
4. Réciproquement, utiliser la cyclicité du groupe multiplicatif $\mathbf{Z}_p^*$ pour montrer que si $a^{(p-1)/2} = 1$ alors l'équation $x^2 = a$ a au moins une solution dans $\mathbf{Z}_p$ (si g est un générateur de $\mathbf{Z}_p^*$ et $a = g^m$, montrer d'abord que m est pair, puis chercher alors à quelle condition $X \in \mathbf{Z}$ est tel que $x = g^X$ est solution de $x^2 = a(= g^m)$).
5. Supposons de plus que $p \equiv 3 \pmod 4$ et soit $a \in \mathbf{Z}_p^*$ tel que $a^{(p-1)/2} = 1$. Montrer que les solutions $x \in \mathbf{Z}_p$ de l'équation $x^2 = a$ sont $x = \pm a^{(p+1)/4}$.
6. On choisit $p = 103$ et $a = [2]_{103}$ et on pose $x_k = a^{2^k}$. Calculer x_0, x_1, x_2, x_3, x_4 et x_5 (présenter le résultat sous forme de tableau), puis $a^{(p-1)/2} = a^{51}$ et $b := a^{(p+1)/4} = a^{26}$, et vérifier que $b^2 = 2$.

Faculté des Sciences de Luminy
Année 2002/2003

DEUG 2 MIAS + MASS MF & SE
Option : Arithmétique. Examen de Juin 2003
Aucun document autorisé. Calculatrice autorisée. Durée : 3 heures

Exercice 1. Montrer (très correctement!) que si $a \geq 1$ et $b \geq 1$ entiers sont tels que $\mathrm{pgcd}(a, b) = 1$, alors $\mathrm{pgcd}(a + b, ab) = 1$.

Exercice 2. Montrer que si n_1 et n_2 sont premiers entre eux et divisent tous deux n, alors le produit $n_1 n_2$ divise également n.

Exercice 3. Résoudre (en expliquant très clairement ce que l'on fait) le système de congruences

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 5 \pmod{25}, \end{cases}$$

c'est à dire donner x_0 tel que x vérifie la congruence précédente si et seulement si $x \equiv x_0 \pmod{12 \cdot 25}$. Résoudre ensuite le système de congruences

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 5 \pmod{25} \\ x \equiv 1 \pmod{77}, \end{cases}$$

c'est à dire donner x_0' tel que x vérifie la congruence précédente si et seulement si $x \equiv x_0' \pmod{12 \cdot 25 \cdot 77}$.

Exercice 4.
4.1. Soient $n > 1$ entier et a premier à n. Expliquer pourquoi $[a]_n^{\phi(n)-1}$ est l'inverse de $[a]_n$ dans le groupe multiplicatif $\mathbf{Z}_n^*$.
4.2. En déduire que $[73]_{132}^{39}$ est l'inverse $[73]_{132}$ dans $\mathbf{Z}_{132}^*$.
4.3. Écrire 39 en base 2 puis, en donnant la table des $x_i := [73]_{132}^{2^i}$ pour $0 \leq i \leq 5$, calculer $[73]_{132}^{-1}$ (et vérifiez votre résultat !).
4.4. En déduire des entiers relatifs u et v tels que $73u - 132v = 1$.

Exercice 5. Montrer que si $p > 2$ premier divise un entier de la forme $n^{2^k} + 1$ (avec $n \geq 1$ entier) alors $p \equiv 1 \pmod{2^{k+1}}$ (calculer l'ordre de $[n]_p$ dans $\mathbf{Z}_p^*$).

Exercice 6. Pour $n \geq 2$ entier on factorise

$$2^n - 1 = \prod_{p | 2^n - 1} p^{e_p}$$

où $p \geq 3$ parcourt les diviseurs premiers de $2^n - 1$. On pose

$$u_n = \prod_{\substack{p | 2^n - 1 \\ e_p = 1}} p \text{ et } v_n = \prod_{\substack{p | 2^n - 1 \\ e_p \geq 2}} p^{e_p},$$

de sorte que $2^n - 1 = u_n v_n$, p divise u_n implique p^2 ne divise pas $2^n - 1$, et p divise v_n implique p^2 divise $2^n - 1$.
6.1. Soit $p \geq 3$ premier divisant u_n.
A. Montrer que l'ordre d de $[2]_p$ dans le groupe multiplicatif $\mathbf{Z}_p^*$ divise $p - 1$ et n.
B. On écrit $2^d = 1 + kp$. Pourquoi est-ce possible? Montrer qu'alors

$$2^{p-1} \equiv 1 + k\frac{p-1}{d}p \pmod{p^2}$$

et

$$2^n \equiv 1 + k\frac{n}{d}p \pmod{p^2},$$

et en déduire que $2^{p-1} \not\equiv 1 \pmod{p^2}$.
6.2. Montrer que si $\lim_{n \to +\infty} u_n = +\infty$, alors il existe une infinité de nombres premiers $p \geq 3$ tels que $2^{p-1} \not\equiv 1 \pmod{p^2}$ (en expliquant pourquoi si il n'en existe qu'un nombre fini alors u_n est majoré indépendamment de n).

Exercice 7. Pour $n \geq 2$ et $a > b \geq 1$ entiers, on pose

$$N = N(n, a, b) := (a^n - b^n)/(a - b).$$

7.1. Montrer que $N(n, a, b)$ est un entier, que si $n = n_1 n_2$ alors $N(n_1, a, b)$ divise $N(n, a, b)$, et que si n n'est pas premier alors N n'est pas non plus premier.
7.2. On suppose $n \geq 2$ premier. Montrer que si $p \geq 2$ premier ne divisant ni a ni b ni $a - b$ divise $N(n, a, b)$, alors $p \equiv 1 \pmod{n}$ (commencer par montrer que $g := [a]_p [b]_p^{-1} \in \mathbf{Z}_p^*$ est bien défini, puis déterminer son ordre dans le groupe multiplicatif $\mathbf{Z}_p^*$).
7.3. Factoriser $N(11, 3, 1) = (3^{11} - 1)/2 = 88573$.

Faculté des Sciences de Luminy
Année 2002/2003

DEUG 2 MIAS + MASS MF & SE
Option : Arithmétique. Examen de Septembre 2003
Aucun document autorisé. Calculatrice autorisée. Durée : 3 heures

Exercice 1. Donner l'ordre de $g = [2]_{17}$ dans le groupe multiplicatif $\mathbf{Z}_{17}^*$. Ce groupe est-il cyclique ?

Exercice 2. Donner l'ordre du groupe multiplicatif $\mathbf{Z}_{315}^*$.

Exercice 3. Utiliser l'algorithme d'Euclide pour calculer $d := \text{pgcd}(73, 59)$. "Remonter" alors cet algorithme pour trouver u et v entiers relatifs tels que $u \cdot 73 - v \cdot 59 = d$ (Bézout). En déduire $[59]_{73}^{-1}$ dans $\mathbf{Z}_{73}^*$.

Exercice 4. Soit $(F_n)_{n\geq 0}$ la suite d'entiers définie par récurrence par $F_1 = F_0 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour $n \geq 0$. On définit alors les matrices colonnes V_n par

$$V_n := \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} \quad (n \geq 0).$$

1. Soit $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Montrer par récurrence sur $n \geq 0$ que

$$V_n = A^n V_0.$$

2. Soit $A_k := A^{2^k}$, $k \geq 0$. Que vaut A_0? Exprimer A_{k+1} à partir de A_k.
3. Calculer alors A^{64} modulo 11 (disposer les calculs matriciels requis de manière à limiter le nombre de matrices à écrire).
4. En déduire V_{64} modulo 11, puis F_{64} modulo 11.

Exercice 5. Soient $a \geq 1$ et $b \geq 1$ entiers.
(i) Montrer que si $\mathrm{pgcd}(a, b) > 1$ alors il existe $p \geq 2$ premier divisant a et b. Montrer alors
(iia) que si $\mathrm{pgcd}(a, b) = 1$ alors pour $k \geq 1$ et $l \geq 1$ on a $\mathrm{pgcd}(a^k, b^l) = 1$ (utiliser le Lemme d'Euclide pour monter que si $\mathrm{pgcd}(a^k, b^l) > 1$ alors $\mathrm{pgcd}(a, b) > 1$),
(iib) et que si $\mathrm{pgcd}(a, b) = 1$ alors $\mathrm{pgcd}(a + b, ab) = 1$ (utiliser le Lemme d'Euclide pour monter que si $\mathrm{pgcd}(a + b, ab) > 1$ alors $\mathrm{pgcd}(a, b) > 1$).

Exercice 6. Soit $k \geq 2$ fixé. Montrer que si $uv = n^k$ et $\mathrm{pgcd}(u, v) = 1$, alors il existe n_1 et n_2 premiers entre eux tels que $n = n_1 n_2$, $u = n_1^k$ et $v = n_2^k$ (on pourra faire une récurrence sur $n \geq 1$ en remarquant que si p premier divise $n > 1$ alors p divise u et est premier avec v (ou l'inverse), puis que p^k est premier avec v et divise u, et en déduire que $u'v' = n'^k$ avec $u' = u/p^k$, $v' = v$ et $n' = n/p$).

Exercice 7. Soient $p \equiv 3 \pmod 4$ premier, $q := (p - 1)/2$ (qui est donc impair) et g un générateur du groupe cyclique $\mathbf{Z}_p^*$ d'ordre $p - 1$.
a). Que vaut $g^q = g^{(p-1)/2}$?
b). Montrer que $y = g^k$ vérifie $y^2 = 1$ si et seulement si $(p - 1)/2$ divise k, et que $x = g^k$ vérifie $x^4 = 1$ si et seulement si $(p - 1)/2$ divise k. En déduire toutes les solutions de $y^2 = 1$ et $x^4 = 1$ dans $\mathbf{Z}_p^*$.
c). Montrer que l'image $\mathrm{Im}(f)$ de $f : \mathbf{Z}_p \longrightarrow \mathbf{Z}_p$ définie par $f(x) = x^4 - 17$ et l'image $\mathrm{Im}(g)$ de $g : \mathbf{Z}_p \longrightarrow \mathbf{Z}_p$ définie par $g(y) = 2y^2$ sont de même cardinal $\#\mathrm{Im}(f) = \#\mathrm{Im}(g) = (p + 1)/2$ (regarder quand $f(x_1) = f(x_2)$ et quand $f(y_1) = f(y_2)$).
d). Expliquer pourquoi $\mathrm{Im}(f) \cap \mathrm{Im}(g) \neq \emptyset$.
e). En déduire que pour tout $p \equiv 3 \pmod 4$ premier il existe x et y dans $\mathbf{Z}_p$ tels que $x^4 - 17 = 2y^2$.

Faculté des Sciences de Luminy
Année 2003/2004

DEUG 2 MIAS + MASS MF & SE
Option : Arithmétique. Examen du 7 Juin 2004
Aucun document autorisé. Calculatrice autorisée. Durée : 3 heures

Exercice 1. Soient $a \geq 1$ et $b \geq 1$ entiers. Montrer que si p premier divise ab et $a + b$, alors p divise a et b. Qu'en déduit-on pour $\mathrm{pgcd}(ab, a + b)$ lorsqu'on suppose que $\mathrm{pgcd}(a, b) = 1$?

Exercice 2. Utiliser le Lemme d'Euclide pour montrer que si $\mathrm{pgcd}(a, b) = 1$ alors $\mathrm{pgcd}(a^k, b^l) = 1$ pour tous $k \geq 1$ et $l \geq 1$.

Exercice 3. Utiliser l'algorithme d'Euclide pour déterminer $d = \text{pgcd}(122, 71)$ et u et v tels que $122u - 71v = d$.

Exercice 4. Soient $p \geq 2$ premier et $a \in \mathbf{Z}$ non divisible par p. Expliquer pourquoi $[a]_p^{p-2}$ est l'inverse de $[a]_p$ dans le groupe multiplicatif $\mathbf{Z}_p^*$. On choisit $p = 101$ et $a = 7$. En écrivant $p - 2 = 99$ en base 2 et en donnant le tableau des $x_k := [7]_{101}^{2^k}$ pour $0 \leq k \leq 6$, déterminer $[7]_{101}^{-1}$, puis en déduire ensuite $u \in \mathbf{Z}$ et $v \in \mathbf{Z}$ tels que $7u - 101v = 1$.

Exercice 5. Soient $p \geq 3$ premier et $n \geq 1$. Montrer que l'équation $x^2 = 1$ n'a que deux solutions dans $\mathbf{Z}_{p^n}$.

Exercice 6. Montrer que pour $p \geq 2$ premier, $x \in \mathbf{Z}_p^*$ est générateur du groupe cyclique $\mathbf{Z}_p^*$ si et seulement si $x^{(p-1)/l} \neq 1$ pour tout $l \geq 2$ premier divisant $p - 1$. Montrer alors que $x = [2]_{101} \in \mathbf{Z}_{101}^*$ est générateur de $\mathbf{Z}_{101}^*$.

Exercice 7.
7.1. Démontrer que tout diviseur premier $q \geq 3$ ne divisant pas $n - 1$ d'un nombre N de la forme

$$N = n^p - 1$$

(avec $p \geq 2$ premier et $n \geq 2$) vérifie $q \equiv 1 \pmod{2p}$.
7.2. Démontrer que tout diviseur premier $p \geq 3$ d'un nombre N de la forme

$$N = m^{2^n} + 1$$

(avec $n \geq 0$ et $m \geq 1$) vérifie $p \equiv 1 \pmod{2^{n+1}}$.

Exercice 8. Soit $p \geq 3$ premier.
8.1. En étudiant l'application

$$f : x \in \mathbf{Z}_p^* \longrightarrow f(x) := x^2 \in \mathbf{Z}_p^*,$$

montrer qu'il y a $(p-1)/2$ carrés dans $\mathbf{Z}_p^*$.
8.2. Montrer que tout carré de $\mathbf{Z}_p^*$ est racine du polynôme $x^{(p-1)/2} - 1 \in \mathbf{Z}_p[x]$, et en déduire que $x \in \mathbf{Z}_p^*$ est un carré dans $\mathbf{Z}_p^*$ si et seulement si $x^{(p-1)/2} = 1$.
8.3. Retrouver ce résultat en utilisant la cyclicité du groupe multiplicatif $\mathbf{Z}_p^*$.
8.4. Montrer que -1 est un carré dans $\mathbf{Z}_p^*$ si et seulement si $p \equiv 1 \pmod{4}$.

Faculté des Sciences de Luminy
Année 2003/2004

DEUG 2 MIAS + MASS MF & SE
Option : Arithmétique. Examen Septembre 2004
Aucun document autorisé. Calculatrice autorisée. Durée : 2 heures

Exercice 1. Soient $a \geq 1$ et $b \geq 1$ entiers. Montrer que si p premier divise ab et $a + b$, alors p divise a et b. Qu'en déduit-on pour $\text{pgcd}(ab, a + b)$ lorsqu'on suppose que $\text{pgcd}(a, b) = 1$? A t-on toujours $\text{pgcd}(ab, a + b) = \text{pgcd}(a, b)$?

Exercice 2. Soient $n \geq 2$ entier et $a \in \mathbf{Z}$ premier à n. Expliquer pourquoi $[a]_n^{\phi(n)-1}$ est l'inverse de $[a]_n$ dans le groupe multiplicatif $\mathbf{Z}_n^*$. On choisit $n = 165 = 3 \cdot 5 \cdot 11$ et $a = 7$. En écrivant $\phi(n) - 1 =$? en base 2 et en donnant le tableau des $x_k := [7]_{165}^{2^k}$ pour $0 \leq k \leq 6$, déterminer $[7]_{165}^{-1}$, puis en déduire ensuite $u \in \mathbf{Z}$ et $v \in \mathbf{Z}$ tels que $7u - 165v = 1$.

Exercice 3. Démontrer que tout diviseur premier $q \geq 3$ ne divisant pas $n-1$ d'un entier N de la forme

$$N = n^p - 1$$

(avec $p \geq 3$ premier et $n \geq 2$) vérifie $q \equiv 1 \pmod{2p}$. Factoriser alors en produit de premiers l'entier $N = 3^{11} - 1 = 177\,146$.

Exercice 4. Résoudre (en expliquant très clairement ce que l'on fait) le système de congruences

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 5 \pmod{25}, \end{cases}$$

c'est à dire donner x_0 tel que x vérifie la congruence précédente si et seulement si $x \equiv x_0 \pmod{12 \cdot 25}$. Résoudre ensuite le système de congruences

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 5 \pmod{25} \\ x \equiv 1 \pmod{77}, \end{cases}$$

c'est à dire donner x_0' tel que x vérifie la congruence précédente si et seulement si $x \equiv x_0' \pmod{12 \cdot 25 \cdot 77}$.

Faculté des Sciences de Luminy
Année 2004/2005

L2. Option : Algèbre et Arithmétique. Examen du 19 Janvier 2005
Aucun document autorisé. Calculatrice autorisée. Durée : 3 heures

Exercice 1. Décomposer en éléments simples sur $\mathbf{C}$ la fraction rationnelle

$$f(X) = \frac{1}{(1-X^2)(1-X^3)}$$

(on posera $j = \exp(2\pi i/3) = (-1 + i\sqrt{3})/2$ et on remarquera que $j^2 = \exp(4i\pi/3) = \bar{j} = (-1 - i\sqrt{3})/2$). Développer alors $f(X)$ en série formelle $f(X) = \sum_{n \geq 0} a_n X^n$. En déduire finalement une formule pour le nombre de manière de décomposer un entier $n \geq 0$ sous la forme $n = 2a + 3b$ avec $a \geq 0$ et $b \geq 0$ entiers. Vérifier votre formule pour $n = 5$ et $n = 17$.

Exercice 2. Soit $n > 1$ entier. Redémontrer le résultat fondamental de cours selon lequel $[a]_n \in \mathbf{Z}_n$ est inversible dans cet anneau unitaire (i.e. que $[a]_n \in \mathbf{Z}_n^*$) si et seulement si $\mathrm{pgcd}(a, n) = 1$, et donner un moyen efficace (pour n grand) du calcul de l'inverse $[a]_n^{-1}$ dans le groupe multiplicatif $(\mathbf{Z}_n^*, \cdot)$. Application, donner l'inverse de $[23]_{101}$ dans $\mathbf{Z}_{101}$ (penser à vérifier votre résultat).

Exercice 3. Soit $n > 2$ entier. Rappelons (voir exercice 2) que

$$\phi(n) := \#\{a;\ 1 \leq a \leq n \text{ et } \mathrm{pgcd}(a, n) = 1\} = \mathrm{Card}(\mathbf{Z}_n^*).$$

Montrer que si $\phi(n) = p \geq 2$ est premier alors tout $g \in G = \mathbf{Z}_n^*$ avec $g \neq 1_G = [1]_n$ est d'ordre p. En choisissant $g = [n-1]_n = [-1]_n$, en déduire qu'il n'existe pas de $n > 2$ tel que $\phi(n)$ soit un nombre premier impair $p \geq 3$. Adapter votre raisonnement pour montrer que $\phi(n)$ est toujours pair pour $n > 2$.

Exercice 4. Soit $(F_n)_{n \geq 0}$ la suite à termes entiers définie par $F_0 = F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$, $n \geq 0$. Soient $p = 11$ et $(f_n)_{n \geq 0}$ la suite à termes dans $\mathbf{Z}_{11}$ définie par $f_n = [F_n]_{11}$. Faire le tableau des valeurs de f_n pour $0 \leq n \leq 12$. En déduire que $(f_n)_{n \geq 0}$ est périodique de période 10. Calculer alors F_{1024} modulo 11.

Exercice 5. Soit $p > 3$ premier divisant $N_q = 2^q + 1$ avec $q \geq 2$ premier. Montrer que $g = [2]_p \in \mathbf{Z}_p^*$ est d'ordre $2q$ dans le groupe multiplicatif $G = \mathbf{Z}_p^*$. En déduire que $p \equiv 1 \pmod{2q}$. Application : factoriser $N_{13} = 8193$.

Exercice 6. Soit $p \geq 3$ premier divisant $2^m - 1$ et $2^n - 1$, avec $m \geq 2$ et $n \geq 2$ entiers. En regardant l'ordre de $g = [2]_p \in \mathbf{Z}_p^*$, montrer que $\mathrm{pgcd}(m, n) > 1$. Que peut-on alors dire de $\mathrm{pgcd}(2^m - 1, 2^n - 1)$ lorsque $\mathrm{pgcd}(m, n) = 1$?

Exercice 7. Montrer en utilisant le Lemme d'Euclide que pour $p \geq 3$ premier l'équation $x^2 = [1]_p$ n'a que les deux solutions $x = [1]_p$ et $x = [-1]_p$ dans $\mathbf{Z}_p$. Donner dans $\mathbf{Z}_8$ toutes les solutions de l'équation $x^2 = [1]_8$.

Exercice 8. Soit $q \geq 1$ premier fixé.
8.1. Montrer que si $p \geq 2$ premier avec $p \neq q$ divise un entier N de la forme

$$N = 1 + y + y^2 + \cdots + y^{q-1}$$

(avec $y \geq 1$ entier), alors $g = [y]_p$ est d'ordre q dans le groupe $G = \mathbf{Z}_p^*$ (remarquer que $(1 - y)N = 1 - y^q$). En déduire que $p \in \{qk + 1;\ k \geq 0\}$.
8.2. En déduire que la progression arithmétique $\{qk + 1;\ k \geq 0\}$ contient au moins un puis une infinité de nombres premiers (pour en construire un premier p_1, choisir $y = q$; si $3 \leq p_1 < \cdots < p_n$ sont $n \geq 1$ premiers distincts de cette progression, choisir $y = qp_1p_2 \cdots p_n$ pour en construire un $n + 1$ième p_{n+1} distinct de ceux-ci).