Première partie

Algèbre générale

1 Arithmétique dans $\mathbb{Z}$

1.1 Division dans $\mathbb{Z}$

1.1 Définition. Soient $a, b \in \mathbb{Z}$. On dit que a divise b et on écrit $a|b$ s'il existe $c \in \mathbb{Z}$ tel que $b = ac$.

On dit aussi que b est un multiple de a, que b est divisible par a, que a est un diviseur de b...

1.2 Propriétés élémentaires. a) Pour tout $a \in \mathbb{Z}$, on a : $1|a$, $a|a$ et $a|0$.

b) Pour tout $a, b \in \mathbb{Z}$, on a : ($a|b$ et $b|a$) $\iff$ $|a| = |b|$.

c) Pour tout $a, b, c \in \mathbb{Z}$, on a : ($a|b$ et $b|c$) $\Rightarrow$ $a|c$.

d) Pour tout $a, b, c \in \mathbb{Z}$, on a : ($a|b$ et $a|c$) $\Rightarrow$ $a|b + c$.

1.3 Exercice. a) Soient $a, b, c, d \in \mathbb{Z}$. Démontrer que si $a|b$ et $c|d$ alors $ac|bd$.

b) Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$. Démontrer que si $a|b$, alors $a^n|b^n$.

1.4 Théorème : Division euclidienne. *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}$ non nul. Alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tels que $a = bq + r$ et $0 \leqslant r < b$.*

1.5 Définition. Un nombre $p \in \mathbb{Z}$ est dit *premier* s'il a exactement 4 diviseurs : $1, p, -1$ et $-p$.

En particulier, 1 (et -1) n'est pas (ne sont) pas premier(s).

1.6 Proposition. *Soit $n \in \mathbb{Z}$ un nombre distinct de 1 et de -1. Alors n admet un diviseur premier.*

Le plus petit diviseur strictement supérieur à 1 de n est un nombre premier.

1.7 Théorème. *Il y a une infinité de nombres premiers.*

Il suffit en effet de remarquer que tout diviseur premier de $n! + 1$ est $\geqslant n + 1$.

1.2 Sous-groupes additifs de $\mathbb{Z}$

1.8 Notation. Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a, c'est à dire l'ensemble $\{ab;\ b \in \mathbb{Z}\}$ est noté $a\mathbb{Z}$.

1.9 Remarque. Pour $a, b \in \mathbb{Z}$ on a l'équivalence entre :

$$\text{(i) } a|b; \qquad \text{(ii) } b \in a\mathbb{Z} \qquad \text{et} \quad \text{(iii) } b\mathbb{Z} \subset a\mathbb{Z}.$$

D'après 1.2.a), on a $a\mathbb{Z} = b\mathbb{Z}$ si et seulement si $|a| = |b|$ (*i.e.* $b = \pm a$).

1.10 Proposition. *Pour tout $a \in \mathbb{Z}$, l'ensemble $a\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$. C'est le plus petit sous-groupe de $\mathbb{Z}$ contenant a.*

1.11 Théorème. *Tout sous-groupe de $\mathbb{Z}$ est de cette forme : si $G \subset \mathbb{Z}$ est un sous-groupe additif, il existe (un unique) $a \in \mathbb{N}$ tel que $G = a\mathbb{Z}$.*

1.3 PGCD, PPCM algorithme d'Euclide

1.12 Corollaire. *Soient $a, b \in \mathbb{Z}$.*

a) *Il existe un unique $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Le nombre m est un multiple commun de a et de b. Les multiples communs de a et b sont les multiples de m.*

b) *Il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Le nombre d est un diviseur commun de a et de b. Les diviseurs communs de a et b sont les diviseurs de d.*

1.13 Définition. Le nombre d de ce corollaire s'appelle le plus grand commun diviseur (PGCD) de a et b ; on le note $pgcd(a, b)$. Le nombre m de ce corollaire s'appelle le plus petit commun multiple (PPCM) de a et b ; on le note $ppcm(a, b)$.

1.14 Remarque. Soient $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n \in \mathbb{Z}$. On définit de même le plus grand commun diviseur d et le plus petit commun multiple m de $x_1, \ldots, x_n$:

- Le nombre $m \in \mathbb{N}$ est un multiple commun des x_i ; les multiples communs des x_i sont les multiples de m. Autrement dit
$$m\mathbb{Z} = x_1\mathbb{Z} \cap x_2\mathbb{Z} \cap \ldots \cap x_n\mathbb{Z} = \bigcap_{i=1}^{n} x_i\mathbb{Z}.$$
- Le nombre $d \in \mathbb{N}$ est un diviseur commun des x_i ; les diviseurs communs des x_i sont les diviseurs de d. On a
$$d\mathbb{Z} = x_1\mathbb{Z} + x_2\mathbb{Z} + \ldots + x_n\mathbb{Z} = \sum_{i=1}^{n} x_i\mathbb{Z}.$$

1.15 Lemme. *Soient $a, b \in \mathbb{Z}$. On suppose que $b \neq 0$. On note r le reste de la division euclidienne de a par $|b|$. On a $pgcd(a, b) = pgcd(b, r)$.*

1.16 Algorithme d'Euclide. Soient $a, b \in \mathbb{N}$. On suppose que $b \neq 0$.

- On pose $r_0 = a$, $r_1 = b$ et on note r_2 le reste de la division euclidienne de a par b.
- Soit $n \in \mathbb{N}$ non nul et supposons r_j construits pour $1 \leqslant j \leqslant n$. Si r_n n'est pas nul, alors on définit r_{n+1} comme le reste de la division euclidienne de r_{n-1} par r_n : $r_{n-1} = q_n r_n + r_{n+1}$. Si r_n est nul, on arrête la construction.

a) La construction s'arrête en un nombre fini d'étapes.

b) Le PGCD de a et b est le dernier reste non nul.

1.17 Remarques. a) On peut majorer le nombre N d'étapes qu'il faut pour trouver le PGCD. Sachant que la suite r_k est strictement décroissante, on trouve évidemment $N \leqslant b$. Mais on peut faire bien mieux !

Remarquons que $r_{N-1} = q_N r_N \geqslant 2r_N$ (puisque et $0 \leqslant r_N < r_{N-1}$), et pour $1 \leqslant k \leqslant N-1$, on a $r_{k-1} = q_k r_k + r_{k+1} \geqslant r_k + r_{k+1}$, de sorte que, par récurrence, $r_{N-k} \geqslant r_N F_{k+2}$, où F_k est le k-ième nombre de Fibonacci (donné par récurrence par les formules $F_0 = 0$, $F_1 = 1$ et $F_{k+1} = F_k + F_{k-1}$ pour $k \geqslant 1$ - on initialise la récurrence avec $k = 0$ et 1 sachant que $F_2 = 1$ et $F_3 = 2$). Rappelons que F_k croît géométriquement : $F_k = \dfrac{\phi^k - (-1)^k \phi^{-k}}{\sqrt{5}}$ où $\phi = \dfrac{1+\sqrt{5}}{2}$ est le nombre d'or. On a donc $b = r_1 \geqslant F_{N+1} > \dfrac{\phi^{N+1} - 1}{\sqrt{5}}$ une estimation pour N logarithmique en b : $N < \dfrac{\ln(1 + b\sqrt{5})}{\ln \phi} - 1$.

b) Pour écrire une relation de Bézout $d = r_N = au + bv$, on peut remonter les opérations : $r_N = r_{N-2} - r_{N-1}q_{N-1} = r_{N-2} - q_{N-1}(r_{N-3} - r_{N-2}q_{N-2}) = (1 + q_{N-1}q_{N-2})r_{N-2} - q_{N-1}r_{N-3}$, puis en écrivant $r_{N-2} = r_{N-4} - r_{N-3}q_{N-3}$ on exprime r_N en fonction de r_{N-3} et r_{N-4}, et on continue... Cela demande de garder en mémoire la suite des quotients q_k.

On peut faire un peu mieux, en écrivant à chaque étape de l'algorithme $r_k = u_k a + v_k b$. On aura $r_{k+1} = r_{k-1} - q_k r_k = (u_{k-1} - q_k u_k)a + (v_{k-1} - q_k v_k)b$. En même temps qu'on trouvera le PGCD, on aura une relation de Bézout !

1.18 Quelques explications sur la suite de Fibonacci. Soient $a, b \in \mathbb{C}$. On considère les suites u_n qui satisfont une propriété de récurrence $u_{n+2} = au_{n+1} + bu_n$. Elles forment un sous-espace vectoriel E de l'espace $\mathbb{C}^{\mathbb{N}}$ des suites complexes. Comme une telle suite est entièrement déterminée par u_0 et u_1, cet espace vectoriel est de dimension 2 (l'application linéaire $(u) \mapsto (u_0, u_1)$ est un isomorphisme de E sur $\mathbb{C}^2$). On cherche une base de E de la forme $u_n = x^n$ (avec $x \in \mathbb{C}$). La suite (x^n) est dans E si et seulement si $x^2 = ax + b$. Si les racines r_1 et r_2 du polynôme $X^2 - aX - b$ sont distinctes, on obtient deux suites indépendantes r_1^n et r_2^n, donc toutes les solutions s'écrivent $u_n = \alpha r_1^n + \beta r_2^n$ (avec $\alpha, \beta \in \mathbb{C}$). Si $r_1 = r_2 = r$, on vérifie que $u_n = nr^n$ est aussi solution ; les solutions s'écrivent donc (si $r \neq 0$) $u_n = (\alpha + n\beta)r^n$ (avec $\alpha, \beta \in \mathbb{C}$).

Dans le cas de la suite de Fibonacci, $a = b = 1$ et les racines du polynôme $X^2 - X - 1$ sont ϕ et $-\phi^{-1}$ où ϕ est le nombre d'or. Donc $F_k = \alpha\phi^k + \beta(-1)^k\phi^{-k}$. On détermine α et β à l'aide des premiers termes.

1.4 Nombres premiers entre eux

1.19 Définition. On dit que a et b sont premiers entre eux si leur plus grand commun diviseur est 1.

Si $a, b \in \mathbb{Z}$, on peut écrire $a = a'd$ et $b = b'd$ où a' et b' sont premiers entre eux et d est le plus grand commun diviseur de a et b.

Soient $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n$ des nombres entiers. On dit que les x_i sont *premiers entre eux dans leur ensemble* si le plus grand commun diviseur de $x_1, \ldots, x_n$ est 1 ; on dit que les x_i sont *premiers entre eux deux à deux*, si pour tout couple d'entiers i, j avec $1 \leqslant i < j \leqslant n$, les nombres x_i et x_j sont premiers entre eux.

1.20 Théorème de Bézout. *Soient $a, b \in \mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

1.21 Théorème de Gauss. *Soient $a, b, c \in \mathbb{Z}$. Si a divise bc et est premier à b, alors a divise c.*

1.22 Corollaire. *Soient $a, b \in \mathbb{Z}$ et p un nombre premier. Si p divise ab alors p divise a ou b.*

1.23 Lemme. *Soient $p_1, \ldots, p_k \in \mathbb{N}$ des nombres premiers distincts deux à deux et $\beta_1, \ldots \beta_k \in \mathbb{N}^*$. Posons $n = \prod_{j=1}^{k} p_j^{\beta_j}$. L'ensemble des diviseurs premiers de n est $\{p_1, \ldots, p_k\}$ et pour tout j, $p_j^{\beta_j}$ divise n et $p_j^{\beta_j+1}$ ne divise pas n.*

1.24 Théorème. *Tout nombre entier admet une décomposition en produit de nombres premiers unique à permutation des termes près.*

On démontre l'existence à l'aide d'une « récurrence forte » sur n. L'unicité résulte du lemme.

1.5 Congruences, l'anneau $\mathbb{Z}/n\mathbb{Z}$

1.25 Définition. Soient $a, b, n \in \mathbb{Z}$. On dit que a est congru à b modulo n et on écrit $a \equiv b\ [n]$ si n divise $b - a$.

1.26 Proposition. *Soit $n \in \mathbb{Z}$. La relation de congruence modulo n est une relation d'équivalence.*

1.27 Lemme. *Soit p un nombre premier. Pour tout entier k tel que $1 \leqslant k \leqslant p - 1$ le coefficient binomial $\binom{p}{k}$ est divisible par p.*

On a $(p - k)\binom{p}{k} = p\binom{p-1}{k}$.

1.28 Petit théorème de Fermat. *Soit p un nombre premier. Pour tout entier k on a $k^p \equiv k\ [p]$. Si k n'est pas divisible par p, alors $k^{p-1} \equiv 1\ [p]$.*

1.29 Théorème de Wilson. *Pour tout nombre premier, on a $(p-1)! \equiv -1\ [p]$.*

1.30 Définition. Soit $n \in \mathbb{Z}$. On note $\mathbb{Z}/n\mathbb{Z}$ le *quotient d'équivalence* pour la relation de congruence modulo n.

Pour $n \in \mathbb{N}^*$, on a $a \equiv b\ [n]$ si et seulement si a et b ont même reste dans la division euclidienne par n ; on en déduit que $\mathbb{Z}/n\mathbb{Z}$ a n éléments (autant que des restes possibles).

1.31 Proposition. *Soit $n \in \mathbb{Z}$. L'addition et la multiplication de $\mathbb{Z}$ passent au quotient et définissent une structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$.*

En d'autres termes, si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors $a + a' \equiv b + b'\ [n]$ et $aa' \equiv bb'\ [n]$.

1.32 Proposition. *Soit $n \in \mathbb{N}^*$. Les propriétés suivantes sont équivalentes.*

(i) *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.*

(ii) *Le nombre n est premier.*

1.33 Proposition. *Soient $n \in \mathbb{Z}$. La classe d'un élément $a \in \mathbb{Z}$ est un élément inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a et n sont premiers entre eux.*

Pour $n \in \mathbb{N}^*$, le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est donc égal au nombre d'entiers $a \in [0, n-1]$ premiers à n. Ce nombre se note $\varphi(n)$. L'application φ ainsi construite s'appelle *l'indicatrice d'Euler.*

Soit p un nombre premier. Tout nombre non divisible par p est premier à p ; on a donc $\varphi(p) = p - 1$. Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$; alors a est premier avec p^n si et seulement si a est premier avec p, *i.e.* s'il n'est pas divisible par p. Les nombres $a \in [0, p^n - 1]$ divisibles par p sont les kp avec $0 \leqslant k < p^{n-1}$. Ils sont au nombre de p^{n-1}. Donc $\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$.

1.34 Remarque. Soient $m, n \in \mathbb{Z}$ deux nombres entiers. On suppose que $m|n$. Pour $a, b \in \mathbb{Z}$, si $a \equiv b\ [n]$, alors *a fortiori* $a \equiv b\ [m]$. On définit une application naturelle $\pi_{m,n} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ qui à la classe de a modulo n associe sa classe modulo m. C'est clairement un homomorphisme d'anneaux.

1.35 Théorème « Chinois ». *Soient m, n deux nombres premiers entre eux. L'application*

$$\begin{array}{rcl} \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ a & \mapsto & (\pi_{m,mn}(a), \pi_{n,mn}(a)) \end{array}$$

est bijective ; c'est un isomorphisme d'anneaux.

En particulier, si m, n sont premiers entre eux on a $\varphi(mn) = \varphi(m)\varphi(n)$.

1.36 Proposition. *Soit $n \in \mathbb{N}$, $n \geqslant 2$. Notons $p_1, \ldots, p_k$ les nombres premiers (positifs et) distincts qui divisent n. On a $\varphi(n) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right)$.*

1.37 Résolution générale de deux équations type. On va donner une méthode générale pour deux équations : un système de congruences et une équation diophantienne. Chacune de ces équations demande d'abord un calcul de plus grand commun diviseur et une « relation de Bézout ».

a) Résoudre l'équation de congruences : $x \equiv a\ [m]$ et $x \equiv b\ [n]$.

- **On suppose que m et n sont premiers entre eux.** Écrivons une relation de Bézout $mu + nv = 1$. Posons $x_0 = mub + nva$. Alors $x_0 - a = mub + (nv - 1)a = mub - mua$ est un multiple de m et $x_0 - b = (mu - 1)b + nva = nv(a - b)$ est un multiple de n. Notre équation devient
$$x \equiv x_0 \ [m] \ \text{ et } \ x \equiv x_0 \ [n],$$
qui est équivalente à $x \equiv x_0 \ [mn]$. L'ensemble de ses solutions est $\{x_0 + mnk;\ k \in \mathbb{Z}\}$.
- **Cas général.** Notons d le plus grand commun diviseur de m et n. Si x est solution de notre équation, comme d divise $x - a$ et $x - b$, alors $d|b - a$. Si a n'est pas congru à b modulo d, alors notre équation n'a pas de solution. Sinon, écrivons $b - a = \ell d$ et écrivons une relation de Bézout $mu + nv = d$. Posons $x_0 = a + \ell mu = a + \ell(d - nv) = b - n\ell v$. C'est une solution de notre équation. Notre équation devient
$$x \equiv x_0 \ [m] \ \text{ et } \ x \equiv x_0 \ [n],$$
qui est équivalente à $x \equiv x_0 \ [M]$ où $M = \dfrac{|mn|}{d}$ est le plus petit commun multiple de m et n. L'ensemble de ses solutions est $\{x_0 + Mk;\ k \in \mathbb{Z}\}$.

b) Résoudre l'équation diophantienne : $ax + by = c$.

On va supposer que a n'est pas nul. Notons d le plus grand commun diviseur de a et b. Écrivons $a = da'$ et $b = db'$ où a' et b' sont deux nombres premiers entre eux, et donnons une relation de Bézout $a'u + b'v = 1$. L'équation devient $d(a'x + b'y) = c$. Si c n'est pas multiple de d, il n'y a pas de solution. Sinon, écrivons $c = dc'$. L'équation devient $a'x + b'y = c' = c'(a'u + b'v)$, soit $a'(x - c'u) = b'(c'v - y)$. Si (x, y) est solution, alors a' divise $b'(c'v - y)$ et est premier avec b', donc il divise $c'v - y$. Écrivons $c'v - y = ka'$. On doit alors avoir : $a'(x - c'u) = a'b'k$, donc $x - c'u = b'k$. L'ensemble des solutions est contenu dans $\{(c'u + b'k, c'v - ka');\ k \in \mathbb{Z}\}$. On vérifie immédiatement que, inversement, pour tout $k \in \mathbb{Z}$, on a $a(c'u + b'k) + b(c'v - ka') = c$.

Remarquons que dans ces deux équations on a trouvé une *solution particulière* et résolu l'*équation homogène associée.* ***Pourquoi ?***

1.6 Exercices

1.6.1 Divisibilité et congruences

1.1 Exercice. 1. Soient $a, b, \delta \in \mathbb{Z}$. On suppose que δ est un diviseur commun de a et b et qu'il existe $u, v \in \mathbb{Z}$ tels que $\delta = au + bv$. Démontrer que le plus grand commun diviseur de a et b est $|\delta|$.

2. Soient $a, b, c \in \mathbb{N}$. Notons d et m le plus grand commun diviseur et le plus petit commun multiple de a et b. Démontrer que le plus grand commun diviseur de ac et bc est dc et que le plus petit commun multiple de ac et bc est mc.

3. Soient $a, b \in \mathbb{N}$. Démontrer que $dm = ab$ où l'on a noté d et m le plus grand commun diviseur et le plus petit commun multiple de a et b respectivement.

1.2 Exercice. 1. Soient $a, b, c \in \mathbb{Z}$. On suppose que a et b sont premiers entre eux, que $a|c$ et $b|c$. Démontrer que $ab|c$.

2. Soient $a, b, c \in \mathbb{Z}$. On suppose que a est premier à b et à c. Démontrer que a est premier à bc.

3. Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.

   a) On suppose que a et b sont premiers entre eux. Démontrer que a et b^n sont premiers entre eux. En déduire que a^n et b^n sont premiers entre eux.

b) Démontrer que le plus grand commun diviseur de a^n et b^n est d^n où d est le plus grand commun diviseur de a et b.

4. Soient $a, b, c \in \mathbb{Z}$ tels que $a|bc$. Démontrer qu'il existe $d, e \in \mathbb{Z}$ tels que $a = de$ et $d|b$ et $e|c$.

1.3 Exercice. *Propriétés arithmétiques à la base de RSA.*
Soient p, q deux nombres premiers distincts, on note N un multiple commun de $p-1$ et $q-1$. Soit $e \in \{1, \dots, N\}$ un entier premier avec N.

1. Montrer qu'il existe un entier $d \in \{1, \dots, N\}$ tel que $ed \equiv 1[N]$.
2. En utilisant le théorème de Fermat, montrer que pour tout entier n, $n^{ed} \equiv n[p]$ et $n^{ed} \equiv n[q]$.
3. En déduire que l'application $C : \{0, \dots, pq-1\} \to \{0, \dots, pq-1\}$ qui à a associe le reste dans la division de a^e par pq est une bijection de $\{0, \dots, pq-1\}$ sur lui-même.

Sur le système de cryptage à clé appelé RSA (Ron Rivest, Adi Shamir, and Leonard Adleman, 1977) :
Je veux pouvoir recevoir des messages chiffrés de telle sorte que je serai seul à pouvoir les déchiffrer. Pour cela

- Je choisis deux nombres premiers p et q grands (environ 100 chiffres chacun), je calcule leur produit n que je rends public, ainsi que la clé de chiffrement e - un nombre premier à $(p-1)(q-1)$.
- Je calcule aussi un nombre d qui est inverse de e modulo $p-1$ et modulo $q-1$; ce nombre je suis le seul à le connaître, ainsi que les nombres p et q qui m'ont permis de le trouver.

Supposons maintenant que vous vouliez m'envoyer de façon secrète un message qui est un nombre a ayant à peu près 200 chiffres, c'est à dire grand mais inférieur à $n = pq$ (ou une suite a_i de tels nombres si votre message est long). Vous m'envoyez juste le nombre b qui est le reste de a^e dans la division par n (ou la suite des $b_i \equiv a_i^e$ modulo n). Pour retrouver le message d'origine, je n'aurai qu'à calculer le reste de b^d (ou b_i^d) modulo n. Ce système repose sur les faits suivants :

1. Il est « relativement rapide » de vérifier qu'un nombre est premier, et il y a beaucoup de nombres premiers : si je donne un nombre m de 100 au hasard, d'après le théorème des nombres premiers, le plus petit nombre premier $p > m$ a beaucoup de chances d'être tel que $p - m$ soit du même ordre que $\ln m \sim 100 \ln 10$. Donc je peux trouver des nombres premiers p et q « rapidement ».
2. Le nombre e est en général choisi petit ($e = 3, 5$ ou 7 sont des choix courants). Le nombre d est par contre grand 200 chiffres...). Élever à la puissance d modulo n un nombre x est une opération « rapide » : cela implique d'élever des éléments de $\mathbb{Z}/n\mathbb{Z}$ au carré $\log_2 d$ ($\simeq 300$) fois et de multiplier des nombres par x au plus $\log_2 d$ fois.
3. Par contre, on ne sait pas trouver le nombre d connaissant n et e sans trouver p et q, et on ne peut pas trouver la décomposition $n = pq$ rapidement.

1.4 Exercice. *Équations Diophantiennes*
Soient $a, b \in \mathbb{N}^*$ des nombres entiers.

1. Soit $c \in \mathbb{Z}$. Quelles sont toutes les solutions de l'équation $ax + by = c$ avec $(x, y) \in \mathbb{Z}$?
   On suppose dorénavant que a et b sont premiers entre eux.
2. Quel est le plus petit entier qui s'écrit de deux façons sous la forme $ax + by$ avec $x, y \in \mathbb{N}$?
3. On suppose que a et b sont tous deux distincts de 1. Notons A l'ensemble des entiers naturels qui ne peuvent s'écrire sous la forme $ax + by$ avec $x, y \in \mathbb{N}$.
   a) Quel est le plus grand élément de A ?
   b) Démontrer que $A = \{|ua - vb|; (u, v) \in \mathbb{N}^2;\ 1 \leqslant u \leqslant b-1;\ 1 \leqslant v \leqslant a-1\}$.
   c) Combien d'éléments a A ?
4. Rappelons qu'au rugby un essai transformé vaut 7 points, un essai non transformé en vaut 5, un drop ou une pénalité 3.
   a) Quel est le plus grand score pour lequel on est sûr qu'il n'a pas été obtenu que par des essais - transformés ou non ?
   b) Quels sont les scores impossibles ?

1.5 Exercice. *Théorème Chinois.* Soient $a, b \in \mathbb{N}^*$. Posons $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$.

1. Ecrire la décomposition de d et m en facteurs premiers en fonction de celle de a et de b. Comparer cette méthode de calcul de pgcd avec l'algorithme d'Euclide.
2. Démontrer qu'il existe a_1, a_2, b_1, b_2 tels que

- $a = a_1 a_2$, $b = b_1 b_2$;
- $a_1 | b_1$, $b_2 | a_2$;
- a_2 et b_1 sont premiers entre eux.

3. Démontrer que $a_1 b_2 = d$ et $a_2 b_1 = m$.
4. En déduire que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est isomorphe à $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

1.6 Exercice. *Jouons avec la suite de Fibonacci.*

1. Écrire les premiers nombres de Fibonacci. Lesquels sont pairs ? multiples de 3 ? multiples de 5 ?
2. a) Démontrer que, si m divise n alors F_m divise F_n.
   b) Démontrer que pour tout n, l'ensemble des $k \in \mathbb{N}$ tel que n divise F_k est de la forme $a\mathbb{N}$ où $a \in \mathbb{N}^*$. *(Utiliser l'exercice 1.7.3).*
3. Soit $p \geqslant 7$ un nombre premier. Notons J la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ à coefficients dans $\mathbb{F}_p$.
   a) On suppose que 5 est un carré modulo p. Démontrer que la matrice J est diagonalisable (dans $\mathbb{F}_p$). En déduire que F_{p-1} est multiple de p.
   b) (**) On suppose que 5 n'est pas un carré modulo p. Notons $K = \{aI_2 + bJ;\ a, b \in \mathbb{F}_p\}$. Démontrer que
      (i) K est un sous-anneau commutatif de $M_2(\mathbb{F}_p)$;
      (ii) l'anneau K est un corps ;
      (iii) l'application $x \mapsto x^p$ est un automorphisme de K ;
      (iv) pour $x \in K$ on a $x^p = x \iff x \in \{aI_2;\ a \in \mathbb{F}_p\}$;
      (v) posant $J' = J^p$, on a $J' \neq J$ et $J'^2 = J' + 1$;
      (vi) on a $J^p = -J^{-1}$;
      (vii) p divise F_{p+1} ; de plus $F_p \equiv F_{p+2} \equiv -1 \ \ [p]$.

1.7 Exercice. *Algorithme d'Euclide et matrices* 2×2.
Soient $a, b \in \mathbb{N}$, avec $0 < a < b$. On effectue l'algorithme d'Euclide : on pose $r_0 = b$, $r_1 = a$, et, supposant r_{j-1} et r_j construits, si $r_j \neq 0$ on note $r_{j-1} = r_j q_j + r_{j+1}$ la division euclidienne de r_{j-1} par r_j. On note n l'entier pour lequel l'algorithme s'arrête de sorte que $r_{n+1} = 0$ et r_n est le $PGCD$ de a, b.

1. Démontrer que $q_n \geqslant 2$.
2. a) Démontrer que, pour tout $k \in \{1, \ldots, n\}$, on a
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} r_1 \\ r_0 \end{pmatrix}.$$
   b) Démontrer qu'il existe des suites $(a_k)_{1 \leqslant k \leqslant n+1}$ et $(b_k)_{1 \leqslant k \leqslant n+1}$ de nombres entiers telles que pour $k \in \{1, \ldots, n\}$ on ait
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} = \begin{pmatrix} a_k & a_{k+1} \\ b_k & b_{k+1} \end{pmatrix}.$$
   c) Démontrer que $a_1 = 0$, $a_2 = 1$, $b_1 = 1$, $b_2 = q_1$ et, pour $2 \leqslant j \leqslant n$, on a $a_{j+1} = a_j q_j + a_{j-1}$ et $b_{j+1} = b_j q_j + b_{j-1}$. En déduire que les suites a_k et b_k sont croissantes et que l'on a $a_{n+1} \geqslant 2a_n$ et $b_{n+1} \geqslant 2b_n$. Dans quel cas a-t-on égalité dans l'une de ces inégalités ?
   d) Démontrer que l'on a $a_k b_{k+1} - a_{k+1} b_k = (-1)^k$ pour $1 \leqslant k \leqslant n$.
   e) Démontrer que l'on a une relation de Bézout $r_n = (-1)^n a_n b + (-1)^{n+1} b_n a$.
3. a) Démontrer que $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^p = \begin{pmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{pmatrix}$ où F_k est le k-ème nombre de Fibonacci.

b) Démontrer que $b_k \geqslant F_k$ et $a_k \geqslant F_{k-1}$.

4. Expliquer en quoi cette méthode permet de trouver « rapidement »le $PGCD$ de a et b et une identité de Bézout $d = au + bv$.
5. On suppose que a et b sont premiers entre eux. Démontrer qu'il existe $n \in \mathbb{N}^*$ une suite $q_1, \ldots, q_n$ de nombres entiers strictement positifs et $u, v \in \mathbb{N}$ tels que $q_n \geqslant 2$ et

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$

6. On suppose qu'il existe une suite $q_1, \ldots, q_n$ de nombres entiers strictement positifs et $u, v \in \mathbb{N}$ tels que $q_n \geqslant 2$ et

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$

Démontrer que a et b sont premiers entre eux et que la suite des quotients successifs de la division euclidienne de b par a est $q_1, q_2, \ldots, q_n$.

1.8 Exercice. *Algorithme de Cornacchia* (**)

1. Soient $a, b \in \mathbb{N}$ tels que $a < b$ et $a^2 + b^2$ soit un nombre premier p.
   a) Démontrer que a et b sont premiers entre eux.
   b) Démontrer qu'il existe $n \in \mathbb{N}^*$, des nombres entiers strictement positifs $q_1, \ldots, q_n$ avec $q_n \geqslant 2$ et des nombres $u, v \in \mathbb{N}$ tels que

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$

   c) Démontrer que $2u \leqslant a$ et $2v \leqslant b$.
   d) Démontrer que $\begin{pmatrix} u & v \\ a & b \end{pmatrix} \begin{pmatrix} u & a \\ v & b \end{pmatrix}$ s'écrit $\begin{pmatrix} x & \ell \\ \ell & p \end{pmatrix}$ où ℓ est l'unique entier tel que $\ell^2 \equiv -1\ [p]$ et $0 \leqslant \ell < p/2$.
2. Soit $p > 2$ un nombre premier tel que -1 est un carré modulo p (*i.e.* congru à 1 modulo 4 - voir exercice 1.11). Supposons qu'on ait trouvé ℓ tel que $0 \leqslant \ell < p/2$ et $\ell^2 = xp - 1$ avec $x \in \mathbb{N}$. Expliquer comment, grâce à l'algorithme d'Euclide, on trouve alors a et b tels que $a^2 + b^2 = p$.

1.6.2 Nombres premiers

1.9 Exercice. *Nombres de Fermat, nombres de Mersenne.*
Pour tout entier $n \geqslant 1$, on note $f_n = 2^n + 1$ et $M_n = 2^n - 1$.

1. Soit $n \geqslant 1$ un entier.
   Démontrer que si M_n est premier, alors n aussi, et que si f_n est premier alors n est une puissance de 2.

   Indication : Remarquer que $X^m - 1$ divise $X^{km} - 1$ et, si k est impair $X^m + 1$ divise $X^{mk} + 1$.

   On pose $F_k = f_{2^k}$.
2. Soient k, ℓ deux nombres entiers avec $k < \ell$. Démontrer que $2^{2^\ell} \equiv 1[F_k]$. En déduire que F_k et F_ℓ sont premiers entre eux.
3. Soit $p > 2$ un nombre premier et soit q un diviseur premier de M_p. Quel est l'ordre de 2 dans le groupe $(\mathbb{F}_q^*, \cdot)$? En déduire que q est de la forme $2kp + 1$.
4. Démontrer que M_{13} est premier.

5. De même soit $\ell \in \mathbb{N}$ et q un diviseur premier de F_ℓ.
   a) Quel est l'ordre de 2 dans le groupe $(\mathbb{F}_q^*, \cdot)$?
   b) En déduire que q est de la forme $2^{\ell+1}k + 1$.
   c) On suppose que $\ell \geqslant 2$. Il résulte de l'exercice 1.12 que 2 est un carré modulo q. En déduire que $2^{\ell+2}$ divise $q - 1$.
   d) Démontrer que le plus petit diviseur de F_5 distinct de 1 est $\geqslant 641$.
   e) En remarquant que $641 = 5^4 + 2^4$, démontrer que $F_5 \equiv 1 - 5^4 2^{28}$ [641].
   f) Démontrer que $641 | F_5$.

1.10 Exercice. *Cas du théorème de Dirichlet.* (*cf.* COMBES. *Algèbre et géométrie* 12.6).

THÉORÈME DE DIRICHLET. *Soient $a, b \in \mathbb{N}^*$ premiers entre eux. Il y a une infinité de nombres premiers congrus à a modulo b.*

Nous étudions ici le cas où $a = 1$.

Le cas $b = 4$: Soit $a \in \mathbb{N}$ et p un diviseur premier de $a^2 + 1$ distinct de 2.

1. Démontrer que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^4 = 1$.
3. Démontrer que $x^2 \neq 1$.
4. En déduire que p est congru à 1 modulo 4.
5. En prenant a sous-la forme $n!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.
6. Démontrer que, pour $n \geqslant 4$, $n! - 1$ a au moins un diviseur premier congru à 3 modulo 4. En déduire qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Le cas $b = 6$ Soit $a \in \mathbb{N}$ et p un diviseur premier de $a^2 + a + 1$ distinct de 3.

1. Démontrer que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^3 = 1$.
3. Démontrer que $x \neq 1$.
4. En déduire que p est congru à 1 modulo 3.
5. En prenant a sous-la forme $n!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 6.
6. Démontrer que, pour $n \geqslant 3$, $n! - 1$ a au moins un diviseur premier congru à 5 modulo 6. En déduire qu'il existe une infinité de nombres premiers congrus à 5 modulo 6.

Le cas $b = 12$: Soit $a \in \mathbb{N}$ et p un diviseur premier de $a^4 - a^2 + 1$.

1. Démontrer que $p \neq 2$ et $p \neq 3$. Démontrer que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^{12} = 1$.
3. Démontrer que $x^4 \neq 1$ et $x^6 \neq 1$.
4. En déduire que p est congru à 1 modulo 12.
5. En prenant a sous-la forme $n!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 12.

Le cas général [**] Pour $n \in \mathbb{N}^*$, on note Φ_n le n-ième polynôme cyclotomique : $\Phi_n = \prod_{0 \leqslant k < n;\ k \wedge n = 1} X - e^{\frac{2ik\pi}{n}}$. Rappelons que $\Phi_n \in \mathbb{Z}[X]$ et que l'on a l'égalité $X^n - 1 = \prod_{d|n} \Phi_d$.

Soient $n \in \mathbb{N}$, $n \geqslant 2$, $a \in \mathbb{N}$ un multiple de n et p un diviseur premier de $\Phi_n(a)$.

1. Démontrer que $\Phi_n(0) = 1$. En déduire que a et p sont premiers entre eux.

2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^n = 1$.
3. Démontrer que le polynôme $X^n - 1$ n'a pas de facteur carré dans $\mathbb{F}_p[X]$.

   Indication : Utiliser la dérivée
4. Soit $d \in \mathbb{N}$ un diviseur de n distinct de n. Démontrer que les polynômes $X^d - 1$ et Φ_n sont premiers entre eux dans $\mathbb{F}_p[X]$. En déduire que $x^d \neq 1$.
5. En déduire que p est congru à 1 modulo n.
6. En prenant a sous-la forme $N!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo n.

1.11 Exercice. *Carrés dans $\mathbb{F}_p$.* (*cf.* COMBES p. 267)
Soit p un nombre premier distinct de 2. Notons $C \subset \mathbb{F}_p^*$ l'ensemble des carrés, *i.e.* l'ensemble des $x \in \mathbb{F}_p^*$ tels qu'il existe $y \in \mathbb{F}_p^*$ avec $x = y^2$.

1. Le cas de -1.
   a) Démontrer que pour tout $x \in C$ il existe un et un seul $c \in \left\{1, \ldots, \dfrac{p-1}{2}\right\}$ tel que x soit la classe de c^2. Combien y a-t-il de carrés dans F_p^* ?
   b) Démontrer que tout $x \in C$, on a $x^{\frac{p-1}{2}} = 1$.
   c) En déduire que, pour $x \in \mathbb{F}_p^*$, on a $x \in C \iff x^{\frac{p-1}{2}} = 1$.
   d) Démontrer que -1 est un carré modulo p si et seulement si p est congru à 1 modulo 4.
2. Le cas de 3.
   a) Soit $P = X^2 + aX + b$ un polynôme à coefficients dans $\mathbb{F}_p$. Démontrer que P a une racine dans $\mathbb{F}_p$ si et seulement si $a^2 - 4b$ est un carré (*i.e.* $a^2 - 4b \in \{0\} \cup C$).
   b) On suppose que $p \notin \{2, 3\}$. Démontrer l'équivalence entre
      (i) $-3 \in C$.
      (ii) Il existe $x \in \mathbb{F}_p^*$, $x^2 + x + 1 = 0$.
      (iii) Il existe x d'ordre 3 dans le groupe $\mathbb{F}_p^*$.
      (iv) $p \equiv 1$ [3] (ce qui signifie encore $p \equiv 1$ [6]).
3. Le polynôme $X^4 + 1$.
   a) Démontrer que si $a, b \in \mathbb{F}_p^* \setminus C$, alors $ab \in C$.
   b) En déduire qu'un au moins des éléments $-1, 2, -2$ est un carré dans $\mathbb{F}_p$.
   c) En écrivant $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - 1)^2 + 2X^2$ en déduire que pour tout p le polynôme $X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$.
   d) Quelle est la décomposition dans $\mathbb{R}[X]$ du polynôme $X^4 + 1$ en polynômes irréductibles ?
   e) En déduire que $X^4 + 1$ est irréductible sur $\mathbb{Q}$ (et sur $\mathbb{Z}$).

1.12 Exercice. *Réciprocité quadratique pour 2, pour 5.*
Soit p un nombre premier.

1. Soit L un corps commutatif de caractéristique p.
   a) Démontrer que $x \mapsto x^p$ est un endomorphisme de corps de L.
   b) Quelles sont les racines du polynôme $X^p - X$ dans L ?
2. On suppose que p est distinct de 2. Soit L une extension de $\mathbb{F}_p$ et $\omega \in L$ tel que $\omega^4 = -1$. Une telle extension existe d'après le corollaire 3.18. Posons $x = \omega + \omega^{-1}$.
   a) Démontrer que $\omega^2 + \omega^{-2} = 0$ et $x^2 = 2$.
   b) Démontrer que les assertions suivantes sont équivalentes :
      (i) Il existe $y \in \mathbb{F}_p$ tel que $y^2 = 2$.

(ii) $x \in \mathbb{F}_p$;

(iii) $x^p = x$;

(iv) $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$;

(v) $p \equiv \pm 1$ [8] ;

3. On suppose que p est distinct de 2 et de 5. Soit L une extension de $\mathbb{F}_p$ et $\omega \in L$ tel que $\omega^5 = 1$ et $\omega \neq 1$ (*i.e.* une racine du polynôme $1 + X + X^2 + X^3 + X^4$ - une telle extension L existe d'après le corollaire 3.18). Posons $x = \omega + \omega^{-1}$.

a) Démontrer que $\omega^2 + \omega^{-2} = -1 - x$ et $x^2 + x - 1 = 0$.

b) Démontrer que les assertions suivantes sont équivalentes :

(i) Il existe $y \in \mathbb{F}_p$ tel que $y^2 = 5$.

(ii) $x \in \mathbb{F}_p$;

(iii) $x^p = x$;

(iv) $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$;

(v) $p \equiv \pm 1$ [5] ;

(vi) La classe de p est un carré modulo 5.

1.13 Exercice. *Racine carrée de -1 dans $\mathbb{F}_p$.*

Soit p un (grand !) nombre premier. Soit $x \in \mathbb{F}_p^*$.

1. Démontrer que x est un carré dans $\mathbb{F}_p$ si et seulement si $x^{(p-1)/2} = 1$. *(Voir exercice 1.11).*
On suppose que x est un carré et on veut trouver une racine carrée de x.
2. On suppose que $p \equiv 3$ [4]. Démontrer que, si x est un carré, alors $x^{\frac{p+1}{4}}$ est une racine carrée de x.
3. On suppose que $p \equiv 1$ [4] et on cherche une racine carrée de -1. On écrit $p - 1 = 2^\ell u$ avec u entier impair.

a) Soit $a \in \mathbb{F}_p^*$; posons $b = a^u$. Démontrer que b est d'ordre 2^k avec $0 \leqslant k \leqslant \ell$.

b) En choisissant a au hasard, quelle est la probabilité que $b = \pm 1$?

c) Expliquer comment trouver une racine carrée de -1 si $b \neq \pm 1$.

1.14 Exercice. 1. *Les nombres premiers sont espacés.* Démontrer que pour tout $n \in \mathbb{N}$, il existe une suite de n nombres consécutifs non premiers (*i.e.* il existe $a \in \mathbb{N}$ tel que les nombres entiers k avec $a \leqslant k \leqslant a + n - 1$ ne soient pas premiers).

Il y a beaucoup de nombres premiers. On désigne par $(p_n)_{n \geqslant 1}$ la suite ordonnée des nombres premiers. On veut démontrer que la série $\displaystyle\sum_{n=1}^{+\infty} 1/p_n$ diverge.

2. On suit Combes (p. 269).
Soit $k \in \mathbb{N}$. Notons $p_1, \ldots, p_k$ les k plus petits nombres premiers et $A_k \subset \mathbb{N}^*$ l'ensemble des nombres entiers dont tous les diviseurs premiers sont $\leqslant p_k$.

a) Démontrer que tout $a \in A_k$ s'écrit sous la forme $a = b^2 p_1^{\varepsilon_1} \ldots p_k^{\varepsilon_k}$ avec $b \in \mathbb{N}$ et $\varepsilon_j \in \{0, 1\}$. En déduire que, pour tout $x \in \mathbb{N}^*$, le nombre d'éléments de A_k inférieurs à x est $\leqslant \sqrt{x} 2^k$.

b) Démontrer que, pour $x \in \mathbb{N}^*$, la proportion d'éléments $\mathbb{N} \setminus A_k$ dans $[1, x]$ est plus petite que $\displaystyle\sum_{p \in \mathcal{P},\ p_k < p \leqslant x} 1/p$.

c) Démontrer que pour $x = 4^{k+1}$ on a $\displaystyle\sum_{p \in \mathcal{P},\ p_k < p \leqslant x} 1/p \geqslant 1/2$. En déduire que la série $\displaystyle\sum_{n=1}^{+\infty} 1/p_n$ diverge.

3. Démontrer que pour tout entier $k \geqslant 1$, $\displaystyle\prod_{i=1}^{k} \frac{p_i}{p_i - 1} \geqslant \sum_{i=1}^{k} \frac{1}{i}$.

4. Démontrer qu'il existe une infinité de nombres premiers comportant au moins un 9 dans leur développement décimal.

D'après le théorème des nombres premiers, $\pi(x)$ est équivalent à $\dfrac{x}{\ln x}$.

1.15 Exercice. *Inégalités de Tchebychef*

1. Pour $N \in \mathbb{Z}^*$ et un nombre premier p, on appelle *valuation* p-adique de N et on note $v_p(N)$ le plus grand entier k tel que $p^k | N$ - de sorte que l'on a $|N| = \displaystyle\prod_p p^{v_p(N)}$.

   Soient $n \in \mathbb{N}$, $n \geqslant 3$ et p un nombre premier.

   a) Démontrer que l'on a $v_p(n!) = \displaystyle\sum_{k=1}^{+\infty} E\big(np^{-k}\big)$ (où E désigne la partie entière).

   b) En déduire que $v_p\binom{2n}{n}$ est le nombre de $k \in \mathbb{N}$ tel que $E\big(2np^{-k}\big)$ soit impair.

   c) Démontrer que
   - $v_p\binom{2n}{n} \leqslant \dfrac{\ln 2n}{\ln p}$.
   - Si $n < p \leqslant 2n$ alors $v_p\binom{2n}{n} = 1$.
   - Si $p \leqslant n < \dfrac{3p}{2}$ alors $v_p\binom{2n}{n} = 0$.

   d) Démontrer que l'on a :

   (i) $\ln\binom{2n}{n} \geqslant (\ln n)(\pi(2n) - \pi(n))$.

   (ii) $\ln\binom{2n}{n} \leqslant (\ln 2n)\Big(\pi(2n/3) + \pi(2n) - \pi(n)\Big) \leqslant (\ln 2n)\pi(2n)$.

2. Soit $n \in \mathbb{N}^*$. Démontrer que $\displaystyle\sum_{k=0}^{n-1}\binom{2n-1}{k} = 2^{2n-2}$. En déduire que $\dfrac{2^{2n-2}}{n} \leqslant \binom{2n-1}{n-1} \leqslant 2^{2n-2}$, puis que $\dfrac{2^{2n-1}}{n} \leqslant \binom{2n}{n} \leqslant 2^{2n-1}$.

3. Démontrer que, pour tout $x \in \mathbb{R}_+$, $x \geqslant 2$, on a

   a) $\pi(2x) - \pi(x) \leqslant \dfrac{2x(\ln 2)}{\ln x}$ et $\pi(x) \leqslant \dfrac{2x(\ln 2)}{\ln x/2}$.

   b) $\pi(x) \geqslant \dfrac{x(\ln 2)}{\ln x} - 1$.