

DM n° 16 (je sais compter !) : Arithmétique

Ce document est à remplir en toute autonomie. Il ne doit pas être discuté avec d'autres personnes.

Le document est à remettre à l'enseignant au plus tard le vendredi 27 juin 2020 à 14h00.

Il est possible de faire plusieurs exercices mais il faut faire au moins un exercice par partie.

Il est possible de faire plusieurs exercices mais il faut faire au moins un exercice par partie.

Il est possible de faire plusieurs exercices mais il faut faire au moins un exercice par partie.

Il est possible de faire plusieurs exercices mais il faut faire au moins un exercice par partie.

Vous faites AU CHOIX l'un des deux problèmes suivants. Vous avez le droit de faire les 2 bien entendu !

Problème 1 – Postulat de Bertrand, théorème de Sylvester

Le but de ce problème est de démontrer le postulat de Joseph Bertrand (1822-1900, mathématicien et économiste français, beau-frère de Charles Hermite), stipulant que pour tout $n \in \mathbb{N}^*$, il existe un nombre premier dans l'ensemble $[n+1, 2n]$. Ce postulat a été démontré en 1850 par Pafnouti Tchebychev (celui des polynômes). La preuve que nous proposons ici est due au mathématicien hongrois Paul Erdős (1913-1996).

Partie I – Majoration du produit des premiers nombres premiers

Soit \mathcal{P} l'ensemble des nombres premiers, et $n \in \mathbb{N}^*$.

1. En comparant $\binom{2n+1}{n}$ et $\binom{2n+1}{n+1}$, montrer que $\binom{2n+1}{n} \leq 2^{2n}$.
2. Montrer que $\prod_{\substack{p \in \mathcal{P} \\ n+1 < p \leq 2n+1}} p$ divise $\binom{2n+1}{n}$
3. En raisonnant par récurrence sur m , montrer que pour tout $m \geq 2$: $\prod_{\substack{p \in \mathcal{P} \\ p \leq m}} p \leq 4^{m-1}$

Partie II – Majoration d'un coefficient binomial

Soit $n \in \mathbb{N}$, $n > 2$.

1. Montrer que pour tout réel positif x , $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\}$.
2. Montrer que pour tout nombre premier p , et tout entier naturel N , la valuation p -adique de $N!$ est

$$v_p(N!) = \sum_{k \geq 1} \left\lfloor \frac{N}{p^k} \right\rfloor$$

(formule de Legendre).

3. En déduire que :
 - (a) pour tout nombre premier p , $p^{v_p(\binom{2n}{n})} \leq 2n$;
 - (b) pour tout nombre premier $p > \sqrt{2n}$, $v_p\left(\binom{2n}{n}\right) \leq 1$
 - (c) pour tout nombre premier p tel que $\frac{2}{3}n < p \leq n$, $v_p\left(\binom{2n}{n}\right) = 0$ (la clé de la preuve, selon Erdős).

4. En déduire que :

$$\binom{2n}{n} \leq (2n)^{\sqrt{2n}} \left(\prod_{\substack{p \in \mathcal{P} \\ \sqrt{2n} < p \leq \frac{2}{3}n}} p \right) \cdot \left(\prod_{\substack{p \in \mathcal{P} \\ n < p \leq 2n}} p \right).$$

Partie III – Démonstration du postulat de Bertrand

Soit $n \in \mathbb{N}$, $n \geq 2$. On suppose dans cette partie que l'ensemble $\llbracket n+1, 2n \rrbracket$ ne contient aucun nombre premier.

1. (a) Montrer que pour tout entier naturel $k < n$, on a $\binom{2n}{k} < \binom{2n}{k+1}$.

(b) En déduire que $\frac{4^n}{2n} \leq \binom{2n}{n}$.

2. En déduire que :

$$\frac{4^n}{2n} \leq (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n}.$$

3. (a) Justifier que pour tout réel $a > 1$, $a + 1 < 2^a$.

(b) Montrer que $2n \leq 2^{6\sqrt[6]{2n}}$.

4. Montrer que, sous l'hypothèse faite en début de partie, pour tout $n \geq 50$, $2^{2n} < 2^{20(2n)^{2/3}}$. En déduire que $n < 4000$.

5. En remarquant que $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$ sont premiers, démontrer que le postulat de Bertrand est vrai pour $n \leq 4000$.

6. Conclure.

Partie IV – Une conséquence du théorème de Sylvester

Le théorème de Sylvester ci-dessous constitue une généralisation du postulat de Bertrand : Si n et k sont deux entiers strictement positifs tels que $n \geq 2k$, alors l'un au moins des nombres $n, n-1, \dots, n-k+1$ possède un diviseur premier strictement plus grand que k .

1. Montrer que le théorème de Sylvester pour $n = 2k$ est équivalent au postulat de Bertrand.

Dans la suite du problème, on admet le théorème de Sylvester, et on en donne une conséquence assez inattendue : les coefficients binomiaux ne sont presque jamais des puissances. Plus précisément, l'équation $\binom{n}{k} = m^\ell$ n'a pas de solution entière en m dès lors que $\ell \geq 2$ et $4 \leq k \leq n-4$. La preuve exposée ci-dessous est également due à Erdős.

2. Justifier qu'on peut se limiter à l'étude du cas où $n \geq 2k$. On suppose désormais cette condition satisfaite.

3. Montrer que $\binom{n}{k}$ possède un facteur premier $p > k$.

4. Soit n, k dans \mathbb{N}^* tels que $n \geq 2k$. Supposons qu'il existe un entier m , et un entier $\ell \geq 2$ tels que $\binom{n}{k} = m^\ell$

(a) Montrer qu'il existe un entier premier p et un entier $i \in \llbracket 0, k-1 \rrbracket$ tel que p^ℓ divise $n-i$.

(b) En déduire que $n \geq k^\ell$.

5. (a) Justifier l'existence et l'unicité de couples d'entiers positifs (a_i, m_i) , tels que les a_i sont non divisibles par une puissance non triviale d'ordre ℓ , et tels que pour tout $i \in \llbracket 0, k-1 \rrbracket$, $n-i = a_i m_i^\ell$

(b) Montrer que les a_i , $i \in \llbracket 0, k-1 \rrbracket$ sont deux à deux distincts.

Indication : si ce n'est pas le cas, considérer $a_i = a_j$, avec $i < j$. En remarquant que $m_i \geq m_j + 1$, montrer que $(n-i) - (n-j) > \ell \sqrt{a_j m_j^\ell}$, puis que $k > \sqrt{n}$.

6. (La clé de la preuve, selon Erdős)

(a) Montrer qu'il existe u et v des entiers premiers entre eux tels que $u^\ell \prod_{i=0}^{k-1} a_i = v^\ell k!$.

(b) Montrer que tout diviseur premier p de v vérifie $p \leq k$.

(c) Soit p un diviseur premier de v . Montrer que

$$v_p(a_0a_1 \dots a_{k-1}) \leq \sum_{i=1}^{\ell-1} \left(\left\lfloor \frac{k}{p^i} \right\rfloor + 1 \right)$$

(d) À l'aide de la formule de Legendre, en déduire que

$$v_p(v^\ell) \leq \ell - 1.$$

puis que $v = 1$.

(e) Montrer que $\sigma : i \mapsto a_i$ est une bijection de $\llbracket 0, k-1 \rrbracket$ dans $\llbracket 1, k \rrbracket$. On note τ sa réciproque.

7. Montrer que si $\ell = 2$, le résultat attendu est vrai (donc que pour tout $k \geq 4$ et $n \geq 2k$, il n'existe pas de solution entière de l'équation $\binom{n}{k} = m^2$).

8. On suppose $\ell \geq 3$, et $k \geq 4$. Soit $i_1 = \tau(1)$, $i_2 = \tau(2)$ et $i_4 = \tau(4)$.

(a) Montrer que $(n - i_2)^2 \neq (n - i_1)(n - i_4)$

Indication : Poser b, x, y tels que $n - i_2 = b$, $n - i_1 = b - x$, $n - i_4 = b + y$, et montrer que si l'égalité est vraie, $(y - x)b = xy$, puis en minorant $|xy|$, trouver, à l'aide de la question 3, $|xy| > |xy|$.

(b) En déduire que $m_{i_2}^2 \neq m_{i_1}m_{i_4}$.

(c) On suppose $m_{i_2}^2 > m_{i_1}m_{i_4}$. Montrer successivement :

i. $2(k-1)n > (n - i_2)^2 - (n - i_1)(n - i_4) > 4\ell(m_{i_1}m_{i_4})^{\ell-1}$

ii. $2(k-1)nm_{i_1}m_{i_4} > \ell(n-k+1)^2 > 2n^2$ (on pourra remarquer que $n > 6k$)

iii. $kn^{\frac{2}{3}} > n$

(d) Conclure dans le cas où $m_{i_2}^2 > m_{i_1}m_{i_4}$.

(e) Terminer la preuve du résultat.

9. (Question pouvant être traitée séparément ; de la nécessité de l'hypothèse $k \geq 4$)

Soit $(u_n)_{n \in \mathbb{N}}$ définie par $u_0 = 9$ et pour tout $n \in \mathbb{N}$, $u_{n+1} = (2u_n - 1)^2$.

(a) Montrer que pour tout $n \in \mathbb{N}$, $\binom{u_n}{2}$ est un carré parfait.

(b) En déduire que l'équation $\binom{n}{2} = m^2$, d'inconnues entières n et m , admet une infinité de solutions.

(c) Montrer que $\binom{50}{3}$ est un carré parfait. On sait montrer que c'est la seule solution pour $k = 3$ et $\ell = 2$.

Ainsi, l'hypothèse $k \geq 4$ est importante dans la preuve générale. Où s'en est-on servi ?

Problème 2 – Loi de réciprocité quadratique

Le but de ce problème est de démontrer la loi de réciprocité quadratique, due à Gauss. On en présente trois preuves, la première basée sur l'étude de la multiplication par q dans $\mathbb{Z}/p\mathbb{Z}$, la deuxième, due à Eisenstein, basée sur les polynômes de Tchebychev, et la troisième, basée sur l'étude de la signature de certaines permutations, donc sur un argument combinatoire.

Soit p un nombre premier. Un résidu quadratique modulo p est un élément $a \in \mathbb{Z}$ tel qu'il existe $b \in \mathbb{Z}$ tel que $b^2 \equiv a \pmod{p}$. Autrement dit, a est un résidu quadratique si et seulement si sa classe dans $\mathbb{Z}/p\mathbb{Z}$ s'exprime sous forme d'un carré, i.e. est dans l'image de l'application $x \mapsto x^2$.

Pour p un entier premier et a non divisible par p , on définit le symbole de Legendre par

$$\left(\frac{a}{p} \right)_L = \begin{cases} 1 & \text{si } a \text{ est résidu quadratique modulo } p \\ -1 & \text{sinon.} \end{cases}$$

On pose de plus $\left(\frac{a}{p} \right)_L = 0$ si a est divisible par p . Lorsqu'il n'y a pas d'ambiguïté, vous êtes autorisés à écrire plus simplement $\left(\frac{a}{p} \right)$.

La loi de réciprocité quadratique dit alors que si p et q sont deux entiers premiers impairs distincts, alors

$$\left(\frac{q}{p}\right)_L = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right)_L.$$

Les parties II, III et IV sont indépendantes, elles ne dépendent chacune que de la partie I.

Questions préliminaires

Dans ces questions préliminaires, et uniquement dans ces questions, on admet la loi de réciprocité quadratique énoncée ci-dessus.

1. Étant donnés deux entiers premiers impairs, justifier que $\left(\frac{q}{p}\right)_L = \left(\frac{p}{q}\right)_L$, sauf si $p \equiv q \equiv 3[4]$. Quelle relation a-t-on dans ce cas ?
2. Montrer que si $a \equiv b [p]$, alors $\left(\frac{a}{p}\right)_L = \left(\frac{b}{p}\right)_L$.
3. Déterminer $\left(\frac{1}{5}\right)_L$ et $\left(\frac{2}{5}\right)_L$
4. Est-ce que 5 est un résidu quadratique modulo 17 ? Modulo 41 ?

Partie I – Quelques propriétés élémentaires du symbole de Legendre

Dans toute cette partie, p désigne un nombre premier impair.

1. Caractérisation des résidus quadratiques

- (a) Soit n un entier premier avec p . Justifier que $n^{\frac{p-1}{2}} \equiv 1 [p]$ ou $n^{\frac{p-1}{2}} \equiv -1 [p]$
- (b) Justifier que si n est un résidu quadratique premier avec p , $n^{\frac{p-1}{2}} \equiv 1 [p]$.
- (c) En considérant le polynôme $X^{\frac{p-1}{2}} - 1$ de $\mathbb{F}_p[X]$, en déduire que pour tout entier n ,

$$\left(\frac{n}{p}\right)_L \equiv n^{\frac{p-1}{2}} [p] \quad (\text{formule d'Euler})$$

- (d) En déduire enfin la multiplicativité du symbole de Legendre : pour tous entiers m et n ,

$$\left(\frac{mn}{p}\right)_L = \left(\frac{m}{p}\right)_L \left(\frac{n}{p}\right)_L.$$

- (e) En admettant dans cette question (et uniquement dans cette question) la loi de réciprocité quadratique, déterminer $\left(\frac{33}{127}\right)_L$.

2. Lemme de Gauss

Soit m un entier non divisible par p .

- (a) Soit, pour $n \in \llbracket 1, \frac{p-1}{2} \rrbracket$, $r_m(n)$ l'unique représentant de la classe de mn modulo p dans l'intervalle $\llbracket -\frac{p-1}{2}, \frac{p-1}{2} \rrbracket$, et $e_m(n) \in \{-1, 1\}$ son signe. Montrer que les entiers $|r_m(n)|$ sont deux à deux distincts, puis que $n \mapsto e_m(n)r_m(n)$ est une bijection de $\llbracket 1, \frac{p-1}{2} \rrbracket$ dans lui-même.

- (b) En déduire que

$$\left(\frac{m}{p}\right)_L = \prod_{n=1}^{\frac{p-1}{2}} e_m(n) \quad (\text{lemme de Gauss})$$

3. Caractère quadratique de 2

- (a) Déduire du lemme de Gauss que $\left(\frac{2}{p}\right)_L = (-1)^{\lceil \frac{p-1}{4} \rceil}$
- (b) En déduire que $\left(\frac{2}{p}\right)_L = 1$ si $p \equiv \pm 1 [8]$ et $\left(\frac{2}{p}\right)_L = -1$ si $p \equiv \pm 3 [8]$, puis enfin que $\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}$.

Ce résultat est particulièrement important car l'utilisation répétée du théorème de réciprocité quadratique associé à la question préliminaire 2 et à la multiplicativité ramène le calcul des symboles de Legendre au calcul de symboles $\left(\frac{1}{p}\right)_L = 1$ et $\left(\frac{2}{p}\right)_L$.

Partie II – Démonstration calculatoire de la loi de réciprocité quadratique

Soit p et q deux nombres premiers impairs distincts, qu'on se pose pour les 3 parties à venir. Quitte à échanger le rôle de p et q (ce qui n'a pas d'importance, la loi de réciprocité étant symétrique en p et q), on peut supposer que $q > p$. Avec les notations de la partie I, on note μ le cardinal de $\{k \in \llbracket 1, \frac{p-1}{2} \rrbracket \text{ tel que } e_q(k) = -1\}$. On note $s_q(k)$ le reste de la division euclidienne de qk par p .

1. Justifier que $e_q(k)r_q(k) = p \cdot \delta_{-1,e_q(k)} + e_q(k)s_q(k)$, où $\delta_{-1,e_q(k)}$ est le symbole de Kronecker, prenant la valeur 1 si $-1 = e_q(k)$ et 0 sinon.
2. À l'aide d'un résultat de la partie I, justifier que

$$\sum_{k=1}^{\frac{p-1}{2}} p \cdot \delta_{-1,e_q(k)} + e_q(k)s_q(k) = \frac{p^2 - 1}{8}$$

3. Justifier que

$$\sum_{k=1}^{\frac{p-1}{2}} e_q(k) \left(kq - p \left\lfloor \frac{kq}{p} \right\rfloor \right) \equiv q \cdot \frac{p^2 - 1}{8} - pS(q,p) \quad [2],$$

$$\text{où } S(q,p) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor.$$

4. En déduire que $S(q,p) \equiv \mu$ [2], puis que $\left(\frac{q}{p}\right)_L = (-1)^{S(q,p)}$.
 5. En comptant, pour chaque $\ell \in \llbracket 1, \frac{q-1}{2} \rrbracket$, le nombre de termes $\left\lfloor \frac{kq}{p} \right\rfloor$ égaux à ℓ dans la somme définissant $S(q,p)$, montrer que
- $$S(q,p) = \sum_{\ell=1}^{\frac{q-1}{2}} \ell \left(\left\lceil \frac{(\ell+1)p}{q} \right\rceil - \left\lceil \frac{\ell p}{q} \right\rceil \right) = \sum_{\ell=1}^{\frac{q-1}{2}} \ell \left(\left\lfloor \frac{(\ell+1)p}{q} \right\rfloor - \left\lfloor \frac{\ell p}{q} \right\rfloor \right).$$
6. En déduire que $S(q,p) + S(p,q) = \frac{p-1}{2} \cdot \frac{q-1}{2}$. Donner une interprétation géométrique de cette formule, consistant à compter les points entiers dans un certain rectangle.
 7. Démontrer enfin la loi de réciprocité quadratique donnée dans le préambule du problème.

Partie III – Démonstration trigonométrique de la loi de réciprocité quadratique (Eisenstein)

Nous proposons dans cette partie une deuxième démonstration, due à Eisenstein, basée sur l'utilisation des polynômes de Tchebychev. Elle utilise le lemme de Gauss démontré dans la partie I. On se donne un entier naturel impair m , qu'on écrit sous la forme $m = 2n + 1$.

1. Expliciter, sous forme de somme de termes de la forme $a_j X^j (1-X)^{n-j}$, un polynôme P_n de degré n tel que pour tout $x \in \mathbb{R} \setminus n\mathbb{Z}$,

$$P_n(\sin^2(x)) = \frac{\sin(mx)}{\sin(x)}.$$

Déterminer le coefficient dominant de P_n .

2. En déduire que pour tout $x \in \mathbb{R} \setminus \pi\mathbb{Z}$,

$$\frac{\sin(mx)}{\sin(x)} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \left(\sin^2(x) - \sin^2 \frac{2\pi j}{m} \right).$$

3. Montrer qu'avec les notations de la partie I, pour tout $k \in \llbracket 1, \frac{p-1}{2} \rrbracket$,

$$\sin\left(\frac{2\pi}{p}qk\right) = e_q(k) \sin\left(\frac{2\pi}{p}|r_q(k)|\right).$$

4. En déduire la loi de réciprocité quadratique.

Partie IV – Démonstration combinatoire de la loi de réciprocité quadratique

On propose une troisième et dernière démonstration, basée sur l'étude de signatures de certaines permutations.

Soit $m \in \mathbb{Z} \setminus p\mathbb{Z}$, et $\mu_m \in \llbracket 0, p-1 \rrbracket^{\llbracket 0, p-1 \rrbracket}$ définie par $\mu_m(k) = km \pmod{p}$, où $km \pmod{p}$ désigne le reste de la division euclidienne de km par p .

1. Montrer que $\mu_m \in \mathfrak{S}(\llbracket 0, p-1 \rrbracket)$.

On définit alors le symbole de Zolotarev par :

$$\left(\frac{m}{p}\right)_Z = \varepsilon(\mu_m),$$

où ε désigne le morphisme de signature.

On pourra de façon équivalente voir μ_m comme une permutation de $\mathbb{Z}/p\mathbb{Z}$.

2. Montrer que pour tous entiers m et n premiers avec p , $\left(\frac{mn}{p}\right)_Z = \left(\frac{m}{p}\right)_Z \left(\frac{n}{p}\right)_Z$.

3. Montrer que si m est un résidu quadratique p , alors $\left(\frac{m}{p}\right)_Z = 1$

4. Soit $G = \langle m \rangle$ le sous-groupe cyclique du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ engendré par la classe de m , et r son ordre. En considérant les classes modulo G , montrer que le type cyclique de μ_m est $1^1 r^{\frac{p-1}{r}}$, autrement dit que sa décomposition cyclique est composée d'un point fixe et de $\frac{p-1}{r}$ cycles disjoints de longueur r .

5. En déduire une expression de $\varepsilon(\mu_m)$, puis vérifier que $\left(\frac{m}{p}\right)_Z = m^{\frac{p-1}{2}}$. Comparer $\left(\frac{m}{p}\right)_Z$ et $\left(\frac{m}{p}\right)_L$.

6. Comme dans les parties précédentes, q désigne un nombre premier impair distinct de p . Soit $j \in \mathbb{Z}$. Justifier que $i \mapsto qj + j$ est un élément de $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ et déterminer sa signature en fonction de $\left(\frac{q}{p}\right)_Z$.

7. Soit $j \in \llbracket 0, q-1 \rrbracket$ et $\sigma_j : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ définie par :

$$\sigma_j((i, j')) = \begin{cases} (qi + j, j) & \text{si } j = j' \\ (i, j') & \text{sinon} \end{cases}$$

Justifier que σ_j est une permutation de $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, puis déterminer sa signature en fonction de $\left(\frac{q}{p}\right)_Z$.

8. On définit enfin $\sigma \in \mathfrak{S}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})$ par $\sigma(i, j) = (qi + j, j)$ pour tout couple (i, j) cette fois (j n'est plus fixé). Montrer que $\varepsilon(\sigma) = \left(\frac{q}{p}\right)_Z$.

On définit de même $\tau \in \mathfrak{S}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})$ de façon symétrique par $\tau(i, j) = (i, pj + i)$, qui vérifie donc $\varepsilon(\tau) = \left(\frac{p}{q}\right)_Z$.

On définit également $\pi : \mathbb{Z}/pq\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ par $\varphi(\bar{k}) = k \times (1, 1)$, pour $k \in \mathbb{Z}$ et enfin $\lambda : \llbracket 0, pq-1 \rrbracket \rightarrow \llbracket 0, pq-1 \rrbracket$ définie, pour $i \in \llbracket 0, p-1 \rrbracket$ et $j \in \llbracket 0, q-1 \rrbracket$, par $\lambda(qi + j) = pj + i$.

9. Justifier que π est un isomorphisme de groupes, que λ est bien définie et est une permutation, et que

$$\lambda \circ \pi^{-1} \circ \sigma = \pi^{-1} \circ \tau.$$

10. En comptant les inversions, déterminer la signature de λ et démontrer la loi de réciprocité quadratique.