Autour du postulat de Bertrand

Romain Panis *

29 janvier 2018

Dans tout ce qui suit $\mathbb{N}$ désigne l'ensemble des entiers naturels (les entiers positifs), $\mathbb{N}^*$ désigne l'ensemble des entiers naturels privé de 0, $\mathbb{Z}$ désigne l'ensemble des entiers relatifs, $\mathcal{P}$ désigne l'ensemble des nombres premiers, $\mathbb{R}$ désigne l'ensemble des réels et $\mathbb{C}$ désigne l'ensemble des complexes.

On utilisera la notation factorielle : si $n \in \mathbb{N}$, on note

$$n! = n \times (n-1) \times \ldots \times 1$$

avec la convention $0! = 1$. On rappelle de même la définition du coefficient binomial : si $0 \leq k \leq n$, on définit

$$\binom{n}{k} = C_n^k = \frac{n!}{k!(n-k)!}$$

et si $k > n$, on adopte la convention

$$\binom{n}{k} = 0.$$

Si $x \in \mathbb{R}$, on note $\lfloor x \rfloor$ sa partie entière définie comme l'unique entier $k \in \mathbb{Z}$ tel que

$$k \leq x < k+1.$$

On note aussi $\{x\}$ sa partie fractionnaire définie comme l'unique réel de $[0,1[$ vérifiant

$$x = \lfloor x \rfloor + \{x\}.$$

Sauf mention explicite du contraire les lettres n, k désigneront toujours des entiers.

Si $z \in \mathbb{C}$, on note $\mathfrak{R}(z)$ sa partie réelle.

Certaines propriétés algébriques utilisées dans la suite sont rappelées à la fin de ce document.

Introduction

L'objectif de ce cours est d'abord de s'intéresser à quelques résultats génériques concernant les nombres premiers. Il s'agit alors de s'apercevoir que malgré l'extrême simplicité de leur définition, leur répartition au sein des entiers reste un mystère. Bien que Gauss et Euler aient ouvert la voie à l'étude de la répartition des nombres premiers il y a déjà plus de 3 00 ans de cela, certaines questions, déjà posées à l'époque restent aujourd'hui encore sans réponse. Nous nous concentrerons donc sur une introduction à la théorie passionnante et riche qu'est la théorie des nombres. Pour cela, nous choisissons d'étudier le célèbre postulat de Bertrand (qui n'en est plus un depuis Tchebychev) qui donne une information relativement faible sur la localisation des nombres premiers mais qui constitue un premier résultat d'arithmétique non trivial.

*Pour toute information / suggestion concernant ce poly n'hésitez pas à me contacter à **romain.panis@ens.fr**.

1 Quelques outils arithmétiques

On commence par quelques rappels élémentaires.

Définition 2.1 (Divisibilité). *Soient $a, b \in \mathbb{Z}$. On dit que a divise b et on note $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ak$. On dit alors que a est un diviseur de b et que b est un multiple de a.*

Théorème 2.2 (Division euclidienne). Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors, il existe un unique couple $(q, r) \in \mathbb{Z} \times \{0, \dots, b-1\}$ tel que

$$a = bq + r.$$

Preuve.

- On commence par démontrer l'existence de l'écriture ci-dessus. Notons déjà que l'on peut supposer $a \in \mathbb{N}$. En effet, si on arrive à montrer la propriété pour tout $(a, b) \in \mathbb{N} \times \mathbb{N}^*$, alors si $a \in \mathbb{Z} \setminus \mathbb{N}$, on peut écrire $a = -\alpha$ où $\alpha \in \mathbb{N}^*$. Si maintenant $b \geq 1$ est un entier, on a donc $(p, q) \in \mathbb{Z} \times \{0, \dots, b-1\}$ tel que $\alpha = bq + r$. Alors $a = -\alpha = (-q)b - r$. Si $r = 0$ l'écriture convient. Si $r \neq 0$, on écrit

  $$a = (-q+1)b + b - r$$

  et on vérifie que $b - r \in \{0, \dots, b-1\}$. Fixons alors $b \geq 1$ un entier, et considérons aussi $a \in \mathbb{N}$. Notons,

  $$X = \{k \in \mathbb{N}\,,\ kb \leq a\}.$$

  Alors X est une partie non vide ($0 \in X$) et majorée de $\mathbb{N}$ donc admet un plus grand élément noté q. Posons $r = a - qb$ et montrons que $r \in \{0, \dots, b-1\}$. Par définition de q,

  $$qb \leq a < (q+1)b$$

  et donc

  $$0 \leq a - qb < b.$$

  D'où le résultat.
- Montrons l'unicité d'une telle écriture. Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Supposons

  $$a = bq + r = bq' + r'$$

  où $(q, r), (q', r') \in \mathbb{Z} \times \{0, \dots, b-1\}$. Alors,

  $$r - r' = b(q' - q).$$

  Or $r - r' \in \{-b+1, \dots, b-1\}$, donc nécessairement $q = q'$ et $r = r'$.

Définition 2.3. *Soient a et b deux entiers non nuls. On note $a \wedge b$ ou encore* $\mathrm{pgcd}(a, b)$ *le plus grand diviseur commun de a et b. On dit que a et b sont premiers entre eux si $a \wedge b = 1$.*

Remarque 2.4. La notion de pgcd se généralise à n entiers : soient $a_1, \dots, a_n$ des entiers non tous nuls. On note $\mathrm{pgcd}(a_1, \dots, a_n)$ le plus grand diviseur commun des n entiers a_i. Les entiers $a_1, \dots, a_n$ sont dits *premiers entre eux dans leur ensemble* si $\mathrm{pgcd}(a_1, \dots, a_n) = 1$

Exercice 1. Montrer que le pgcd est associatif au sens où : si a, b, c sont trois entiers non nuls,

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c.$$

Proposition 2.5 (Identité de Bézout). *Soient $a, b \in \mathbb{Z}^*$. Notons $a \wedge b = \alpha$. Alors il existe $(u, v) \in \mathbb{Z}^2$ tel que*

$$au + bv = \alpha.$$

Preuve. Notons $X = \{pa + qb\,,\ (p, q) \in \mathbb{Z}^2\} \cap \mathbb{N}^*$. Il s'agit d'une partie de $\mathbb{N}$ contenant $|a|$ (donc non vide). Une partie non vide de $\mathbb{N}$ admettant un minimum, on note

$$d = \min X.$$

On dispose donc de $(u, v) \in \mathbb{Z}^2$ tel que $d = au + bv$. Montrons que $d = \alpha$.

- Déjà, α divise a et b donc divise d ce qui assure que $\alpha \leq d$.
- Montrons que d divise a. On effectue la division euclidienne de a par d : on dispose de $q \in \mathbb{Z}$ et $r \in \{0, \ldots, d-1\}$ tels que $a = qd + r$. On remarque alors que

  $$r = a - qd = a - q(au + bv) = (1 - qu)a + (-qv)b.$$

  En particulier, si jamais $r \neq 0$, on a $r \in X$ et $r < d$ ce qui est impossible par minimalité de d. Donc $r = 0$ et $a = qd$: on en déduit que d divise a. Par symétrie on montrerait de même que d divise b. Ceci assure que $d \leq a \wedge b = \alpha$.

Donc $d = \alpha$ et le couple (u, v) fixé au début convient.

Proposition 2.6 (Lemme de Bézout). *Soient $a, b \in \mathbb{Z}^*$. Alors $a \wedge b = 1$ si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tel que*

$$au + bv = 1.$$

Preuve. Commençons par le sens réciproque et supposons l'existence de $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Soit α un diviseur (strictement positif) commun à a et b. Alors α divise $au + bv$ donc α divise 1 : c'est que $\alpha = 1$. Il vient alors $a \wedge b = 1$. Supposons maintenant $a \wedge b = 1$. L'existence du couple (u, v) voulu découle immédiatement de la proposition 2.5.

Proposition 2.7 (Lemme de Gauss). *Soient a, b, c trois entiers. On suppose que $a \wedge b = 1$ et $a \mid bc$. Alors $a \mid c$.*

Preuve. D'après le lemme de Bézout, on peut trouver $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. On a alors,

$$acu + v(bc) = c.$$

Comme $a \mid bc$ et $a \mid acu$, on a $a \mid c$.

Définition 2.8 (Nombre premier). *Un nombre premier est un entier $p \in \mathbb{N}^*$ qui admet exactement deux diviseurs positifs : 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premier.*

Remarque 2.9.

- Notons que l'on dispose de la définition équivalente suivante d'un nombre premier : un entier $p \in \mathbb{N}^*$ est premier si et seulement si pour tout $(a, b) \in (\mathbb{N}^*)^2$ tel que $p = ab$, on a $a, b \in \{1, k\}$. Ainsi, si un entier $k \geq 2$ n'est pas premier, il se décompose comme le produit de deux entiers supérieurs ou égaux à 2.
- 1 n'est pas un nombre premier : il n'a qu'un seul diviseur positif. 2, 3, 5, 7, 11, 13 sont des nombres premiers.

- Si p et q sont deux nombres premiers distincts, on a $p \wedge q = 1$.
- Le plus grand nombre premier connu à ce jour a été découvert le 26 décembre 2017. Il s'agit d'un nombre de Mersenne (voir exercice 9) : $2^{77232917} - 1$, il comporte (en base 10) 23249425 chiffres !

Proposition 2.10. *Tout entier naturel $n \geq 2$ admet un diviseur premier.*

Preuve. On montre ce résultat par récurrence forte sur $n \geq 2$. Le résultat est vrai pour $n = 2$ (qui est premier). Supposons $n \geq 3$ et le résultat vrai pour tout entier $2 \leq k < n$. Il y a deux possibilités : si n est premier, alors le résultat est immédiat. Sinon n n'est pas premier et s'écrit donc $n = ab$ où $a, b \geq 2$ sont deux entiers. On applique alors l'hypothèse de récurrence à $a < n$ qui admet un diviseur premier : c'est encore un diviseur premier de n. D'où le résultat.

Théorème 2.11 (Euclide). *L'ensemble $\mathcal{P}$ est infini.*

Preuve. Supposons par l'absurde que $\mathcal{P}$ est fini et notons $\mathcal{P} = \{p_1, \dots p_n\}$. Considérons l'entier $N = p_1 \dots p_n + 1$. Comme tout nombre premier est au moins égal à 2, on a $N \geq 2$. D'après la proposition 2.10, N admet un diviseur premier $p_i \in \mathcal{P}$. Ainsi p_i divise N et p_i divise $p_1 \dots p_n$ donc p_i divise 1 ce qui est absurde.

Exercice 2. En reprenant l'idée de la preuve du théorème 2.11, montrer qu'il existe une infinité [1] de nombres premiers de la forme $4k + 3$ où $k \in \mathbb{N}$.

Proposition 2.12. *Soit $p \in \mathcal{P}$. Soient $a_1, \dots, a_n$ des entiers non nuls. On suppose que $p \mid a_1 \dots a_n$. Alors il existe $i \in \{1, \dots, n\}$ tel que $p \mid a_i$.*

Preuve. On raisonne par récurrence sur $n \geq 1$. Pour $n \geq 1$, on note HR_n : " Si $a_1, \dots, a_n$ sont des entiers non nuls tels que $p \mid a_1 \dots a_n$, alors il existe $i \in \{1, \dots, n\}$ tel que $p \mid a_i$".

La propriété est clairement vérifiée au rang $n = 1$. Supposons $n \geq 1$ et la propriété vraie au rang n. Soient $a_1, \dots, a_{n+1}$ des entiers non nuls tels que $p \mid a_1 \dots a_{n+1}$. Si $p \wedge (a_1 \dots a_n) = 1$ alors d'après le lemme de Gauss, $p \mid a_{n+1}$. Sinon, comme p est premier, c'est que $p \mid a_1 \dots a_n$ et on peut appliquer HR_n. Dans les deux cas on aboutit à HR_{n+1}.

Théorème fondamental de l'arithmétique. *Tout entier $n \geq 2$ se décompose de manière unique comme produit de puissances de nombres premiers. Autrement dit, si $n \geq 2$, il existe une unique suite d'entiers positifs $(\alpha_p)_{p \in \mathcal{P}}$ à support fini (c'est à dire nulle à partir d'un certain rang) telle que*

$$n = \prod_{p \in \mathcal{P}} p^{\alpha_p}.$$

1. Un résultat bien plus fort (mais aussi beaucoup plus compliqué...), connu sous le nom de théorème de Dirichlet, assure en fait que si a, b sont deux entiers strictement positifs et premiers entre eux, alors il existe une infinité de nombres premiers de la forme $an + b$ où $n \geq 1$.

Preuve. On commence par montrer l'existence d'une telle décomposition par récurrence forte sur $n \geq 2$. On note donc pour $n \geq 2$, HR_n : "Il existe une suite $(\alpha_p)_{p\in\mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ à support fini telle que $n = \prod_{p\in\mathcal{P}} p^{\alpha_p}$".

Le résultat est vrai pour $n = 2$ en posant $\alpha_2 = 1$ et $\alpha_p = 0$ pour $p \in \mathcal{P} \setminus \{2\}$.

Supposons désormais $n \geq 3$ et HR_2, ..., HR_{n-1} vérifiées. On distingue deux cas :

- Si n est un nombre premier : alors on pose $\alpha_n = 1$ et pour $p \in \mathcal{P} \setminus \{n\}$ on pose $\alpha_p = 0$.
- Sinon, on peut écrire $n = ab$ où $a, b \geq 2$ sont deux entiers. Comme $a, b < n$ on peut appliquer HR_a et HR_b. On dispose alors de deux suites d'entiers à support fini $(\alpha_p(a))_{p\in\mathcal{P}}$ et $(\alpha_p(b))_{p\in\mathcal{P}}$ telles que
$$a = \prod_{p\in\mathcal{P}} p^{\alpha_p(a)}$$
et
$$b = \prod_{p\in\mathcal{P}} p^{\alpha_p(b)}.$$
On a alors
$$n = \prod_{p\in\mathcal{P}} p^{\alpha_p(a)+\alpha_p(b)}.$$
Il suffit alors de poser pour $p \in \mathcal{P}$, $\alpha_p = \alpha_p(a) + \alpha_p(b)$.

Dans tous les cas, on obtient bien HR_n.

Passons à présent à l'unicité d'une telle écriture. Soit $n \geq 2$ un entier. Supposons disposer de deux suites d'entiers $(\alpha_p)_{p\in\mathcal{P}}$ et $(\beta_p)_{p\in\mathcal{P}}$ telles que
$$n = \prod_{p\in\mathcal{P}} p^{\alpha_p} = \prod_{p\in\mathcal{P}} p^{\beta_p}.$$
Supposons par l'absurde qu'il existe $p_0 \in \mathcal{P}$ tel que $\alpha_{p_0} \neq \beta_{p_0}$ et par exemple $\alpha_{p_0} < \beta_{p_0}$. On a alors
$$p_0^{\beta_{p_0}-\alpha_{p_0}} \prod_{p\in\mathcal{P},\, p\neq p_0} p^{\beta_p} = \prod_{p\in\mathcal{P},\, p\neq p_0} p^{\alpha_p}.$$
Par la proposition 2.12, p_0 divise l'un des termes du produit $\prod_{p\in\mathcal{P},\, p\neq p_0} p^{\alpha_p}$: c'est absurde.

Définition 2.13 (Valuation p-adique). *Soient $p \in \mathcal{P}$ et un entier $n \geq 2$. On appelle valuation p-adique de n et on note $v_p(n)$ la plus grande puissance de p divisant n. De cette manière, on peut désormais écrire, pour tout $n \geq 2$,*
$$n = \prod_{p\in\mathcal{P}} p^{v_p(n)}.$$
Notons que cette définition a bien un sens grâce à l'unicité du théorème précédent. On ajoute que l'écriture précédente s'étend à $n = 1$ en choisissant comme convention $v_p(1) = 0$ pour tout $p \in \mathcal{P}$.

Propriétés 2.14. *Soient a, b deux entiers naturels supérieurs ou égaux à 2 et $p \in \mathcal{P}$. On a les résultats suivants :*

(i) $v_p(ab) = v_p(a) + v_p(b)$.

(ii) *Si b divise a, $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$. En particulier comme la valuation p-adique d'un entier est toujours positive ou nulle, on a que si b divise a, pour tout $p \in \mathcal{P}$, $v_p(b) \leq v_p(a)$.*

(iii) $a \wedge b = \prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))}$

(iv) $a \vee b = \prod_{p\in\mathcal{P}} p^{\max(v_p(a),v_p(b))}$

Preuve. On écrit

$$a = \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

et

$$b = \prod_{p \in \mathcal{P}} p^{v_p(b)}.$$

(*i*) Par l'écriture précédente,

$$ab = \prod_{p \in \mathcal{P}} p^{v_p(a)+v_p(b)} = \prod_{p \in \mathcal{P}} p^{v_p(ab)}.$$

L'unicité dans le théorème fondamental de l'arithmétique permet alors d'obtenir pour tout $p \in \mathcal{P}$, $v_p(ab) = v_p(a) + v_p(b)$.

(*ii*) Si b divise a, on écrit

$$\frac{a}{b} = \prod_{p \in \mathcal{P}} p^{v_p\left(\frac{a}{b}\right)} = \prod_{p \in \mathcal{P}} p^{v_p(a)-v_p(b)}.$$

L'unicité dans le théorème fondamental de l'arithmétique permet encore de conclure : pour tout $p \in \mathcal{P}$, $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.

(*iii*) On rappelle que $a \wedge b = \text{pgcd}(a, b)$. Observons déjà que

$$\left(\prod_{p \in \mathcal{P}} p^{\min(v_p(a),v_p(b))}\right) \mid a$$

et

$$\left(\prod_{p \in \mathcal{P}} p^{\min(v_p(a),v_p(b))}\right) \mid b.$$

Si bien que

$$\left(\prod_{p \in \mathcal{P}} p^{\min(v_p(a),v_p(b))}\right) \leq a \wedge b.$$

De même, comme $a \wedge b$ divise a et b on a pour tout $p \in \mathcal{P}$, $v_p(a \wedge b) \leq v_p(a)$ et $v_p(a \wedge b) \leq v_p(b)$ donc

$$v_p(a \wedge b) \leq \min(v_p(a), v_p(b)).$$

On en déduit alors

$$a \wedge b \leq \left(\prod_{p \in \mathcal{P}} p^{\min(v_p(a),v_p(b))}\right)$$

d'où l'égalité recherchée.

(*iv*) On rappelle que $a \vee b = \text{ppcm}(a, b)$. Le raisonnement qui suit est identique à celui développé pour (*iii*). On commence par observer que a et b divisent $\prod_{p \in \mathcal{P}} p^{\max(v_p(a),v_p(b))}$ ce qui impose que

$$a \vee b \leq \prod_{p \in \mathcal{P}} p^{\max(v_p(a),v_p(b))}.$$

On montre l'inégalité réciproque en remarquant que si m est un multiple commun de a et b alors pour tout $p \in \mathcal{P}$, $v_p(m) \geq v_p(a)$ et $v_p(m) \geq v_p(b)$ d'où

$$v_p(m) \geq \max(v_p(a), v_p(b)).$$

En particulier,

$$v_p(a \vee b) \geq \max(v_p(a), v_p(b)).$$

De ceci on tire donc

$$\prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))} \leq a \vee b$$

ce qui donne le résultat voulu.

Remarque 2.15. Notons que si $x, y \in \mathbb{R}$,

$$\max(x, y) = \frac{x + y + |x - y|}{2} \ , \ \min(x, y) = \frac{x + y - |x - y|}{2}$$

et en particulier,

$$\min(x, y) + \max(x, y) = x + y.$$

Avec cette remarque et les points (iii) et (iv) de la proposition précédente, on montre que si $a, b \geq 2$ sont deux entiers,

$$ab = (a \wedge b)(a \vee b).$$

Proposition 2.16 (Formule de Legendre). *Soient $n \geq 2$ un entier et $p \in \mathcal{P}$, alors*

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Preuve. Observons déjà que la somme est bien définie car la suite $\left(\left\lfloor \frac{n}{p^k} \right\rfloor\right)_{k \geq 1}$ est à support fini : si k est tel que $\frac{n}{p^k} < 1$ alors $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$.

Pour montrer la formule voulue on procède ainsi : dans le produit $n!$ il y a $\lfloor \frac{n}{p} \rfloor - \lfloor \frac{n}{p^2} \rfloor$ termes qui sont divisibles par p mais pas par p^2 et ces termes contribuent chacun pour 1 à $v_p(n!)$. Ensuite, il y a $\lfloor \frac{n}{p^2} \rfloor - \lfloor \frac{n}{p^3} \rfloor$ termes divisibles par p^2 mais pas par p^3 et ces termes contribuent chacun pour 2 à $v_p(n!)$. Bout à bout en notant q le premier entier k pour lequel $\lfloor \frac{n}{p^k} \rfloor = 0$, on a

$$v_p(n!) = \sum_{k=1}^{q} \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) k.$$

On en déduit donc

$$v_p(n!) = \sum_{k=1}^{q} \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) k = \sum_{k=1}^{q} \left\lfloor \frac{n}{p^k} \right\rfloor k - \sum_{k=2}^{q+1} \left\lfloor \frac{n}{p^k} \right\rfloor (k-1) = \left\lfloor \frac{n}{p} \right\rfloor + \sum_{k \geq 2} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

D'où la formule recherchée.

Exercice 3. Soient $n \geq 1$, $p \in \mathcal{P}$, $k \in \{1, \ldots, p^n - 1\}$. Calculer $v_p\left(\binom{p^n}{k}\right)$.

Exercice 4. Déterminer par combien de zéros se termine 2018! (Indication : inutile de chercher à utiliser une calculatrice...).

2 Le postulat de Bertrand

On a pu voir dans la partie précédente qu'il existait une infinité de nombres premiers mais on souhaite à présent renforcer un peu ce résultat en précisant légèrement la localisation de ces entiers. On dispose pour cela d'un résultat relativement simple conjecturé par Joseph Bertrand en 1845 et démontré par Pafnouti Tchebychev en 1850. De fait ce résultat porte aujourd'hui le nom de théorème de Tchebychev.

Théorème de Tchebychev. *Soit $n \geq 2$ un entier, alors il existe un nombre premier p vérifiant*

$$n < p < 2n.$$

La preuve qui suit est due à Erdös [E] et se trouve dans [HW]. Le lecteur intéressé par des approches légèrement différentes de ce résultat est invité à consulter la preuve astucieuse de Ramanujan [2] [R]. On détaille en annexe la preuve historique de Tchebychev.

Tout repose sur l'introduction de la fonction θ définie pour $x \in \mathbb{R}$ par

$$\theta(x) = \sum_{p \in \mathcal{P},\, p \leq x} \ln(p).$$

La démonstration qui suit se décompose alors en trois grandes étapes : on commence par prouver un lemme "technique" de majoration de θ, on l'applique pour démontrer le résultat pour les entiers $n > 630$, puis on montre le résultat pour $2 \leq n \leq 630$ en suivant un procédé algorithmique simple connu sous le nom de procédé de Landau.

Lemme (Majoration de θ). *Pour tout $n \in \mathbb{N}^*$, on a*

$$\theta(n) < n \ln(4).$$

Preuve. On raisonne par récurrence forte sur $n \geq 1$ et on note HR_n : "$\theta(n) < n \ln(4)$".

Observons que HR_1 est vraie car $\theta(1) = 0 < 1 \times \ln(4)$. De même pour HR_2 car $\theta(2) = \ln(2) < 2\ln(4)$. Supposons $n \geq 3$ et HR_k vraie pour tout entier $k \in \{2, \ldots, n-1\}$. On distingue deux cas :

- Si n est pair alors n ne peut être premier (car $n > 2$) et donc $\theta(n) = \theta(n-1)$. On applique HR_{n-1} et on obtient,
$$\theta(n) = \theta(n-1) < (n-1)\ln(4) < n\ln(4)$$
ce qui est bien le résultat voulu.
- Si n est impair alors on peut écrire $n = 2m+1$ où $m \in \mathbb{N}^*$. D'après la formule du binôme de Newton, on a
$$4^m = \frac{(1+1)^{2m+1}}{2} = \frac{1}{2}\sum_{k=0}^{2m+1} \binom{2m+1}{k} \geq \frac{1}{2}\left(\binom{2m+1}{m} + \binom{2m+1}{m+1}\right) = \binom{2m+1}{m+1}.$$
De plus si $p \in \mathcal{P}$ est tel que $m+1 < p \leq 2m+1$ alors p divise $\binom{2m+1}{m+1}$ car
$$\binom{2m+1}{m+1} = \frac{(2m+1)\ldots(m+2)}{m!}$$

2. Voir par exemple **http ://vixra.org/pdf/1406.0155v1.pdf**.

et donc $v_p\left(\binom{2m+1}{m+1}\right) = v_p((2m+1)\dots(m+2)) - v_p(m!)$ et comme $p > m$ on a $v_p(m!) = 0$. De ceci, on tire

$$\theta(2m+1) - \theta(m+1) = \sum_{p\in\mathcal{P},\, m+1<p\leq 2m+1} \ln(p) = \ln\left(\prod_{p\in\mathcal{P},\, m+1<p\leq 2m+1} p\right)$$

et par la remarque et la majoration qui précèdent,

$$\theta(2m+1) - \theta(m+1) \leq \ln\left(\binom{2m+1}{m+1}\right) \leq \ln(4^m) = m\ln(4).$$

De plus comme $m+1 < n$ on peut appliquer HR_{m+1} et on a

$$\theta(m+1) < (m+1)\ln(4).$$

Bout à bout, on obtient bien

$$\theta(2m+1) = \theta(n) < n\ln(4).$$

D'où HR_n et le lemme.

Preuve du théorème de Tchebychev pour $n > 630$. L'idée suivante, très astucieuse, est due à Erdös [E]. On commence par observer que si $n \geq 2$,

$$4^n \leq 2n\binom{2n}{n}.$$

En effet, il suffit de d'utiliser la formule du binôme de Newton :

$$4^n = (1+1)^{2n} = 2 + \sum_{k=1}^{2n-1}\binom{2n}{k} \leq 2 + (2n-1)\binom{2n}{n} \leq 2n\binom{2n}{n}.$$

On a utilisé que $2 \leq \binom{2n}{n}$ et si $k \in \{0,\dots,2n\}$, $\binom{2n}{k} \leq \binom{2n}{n}$. On suppose désormais $n > 630$. On note pour $p \in \mathcal{P}$, $\beta(n,p) = v_p\left(\binom{2n}{n}\right)$. Les résultat de la partie II permettent alors d'écrire

$$\binom{2n}{n} = \prod_{p\in\mathcal{P}} p^{\beta(n,p)} = \Lambda_1\Lambda_2\Lambda_3\Lambda_4$$

avec

$$\Lambda_1 = \prod_{p\in\mathcal{P},\, p\leq\sqrt{2n}} p^{\beta(n,p)}$$

$$\Lambda_2 = \prod_{p\in\mathcal{P},\, \sqrt{2n}<p\leq\frac{2n}{3}} p^{\beta(n,p)}$$

$$\Lambda_3 = \prod_{p\in\mathcal{P},\, \frac{2n}{3}<p\leq n} p^{\beta(n,p)}$$

$$\Lambda_4 = \prod_{p\in\mathcal{P},\, n<p<2n} p^{\beta(n,p)}.$$

Cette écriture est bien justifiée puisque $\binom{2n}{n}$ n'admet pas de diviseurs premiers $> 2n$. En effet, il suffit d'écrire si $p \in \mathcal{P}$ et $p > 2n$,

$$v_p\left(\binom{2n}{n}\right) = v_p\left(\frac{(2n)!}{n!n!}\right) = v_p((2n)!) - 2v_p(n!)$$

et on conclut en observant que $v_p((2n)!) = v_p(n!) = 0$ par la formule de Legendre. Ainsi, $\beta(n,p) = 0$ si $p > 2n$. On le voit bien sur l'expression suivante, valable pour $p \in \mathcal{P}$,

$$\beta(n,p) = \sum_{k=1}^{+\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

L'objectif est alors de démontrer la minoration $\Lambda_4 > 1$ qui suffira à conclure (car alors on sait que le produit Λ_4 est indexé par un ensemble non vide). Pour cela on majore Λ_1, Λ_2 et Λ_3.

- Si $k \in \mathbb{N}^*$, on remarque que $\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \in \{0,1\}$. Plus précisément, $\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor = 0$ si $\left\{ \frac{n}{p^k} \right\} < \frac{1}{2}$ et $\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor = 1$ si $\left\{ \frac{n}{p^k} \right\} \geq \frac{1}{2}$. De plus, tous ces termes sont nuls dès que $k > \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor$. Il vient alors pour $p \in \mathcal{P}$,

  $$\beta(n,p) \leq \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor.$$

  Ceci fournit la majoration de Λ_1 suivante :

  $$\Lambda_1 \leq \prod_{p \in \mathcal{P},\, p \leq \sqrt{2n}} p^{\left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor} \leq \prod_{p \in \mathcal{P},\, p \leq \sqrt{2n}} p^{\frac{\ln(2n)}{\ln(p)}} \leq (2n)^{\sqrt{2n}}.$$

- Si à présent $p > \sqrt{2n}$,

  $$\beta(n,p) = \left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor$$

  et comme vu précédemment cette quantité vaut 0 ou 1. Il vient pour $p > \sqrt{2n}$, $\beta(n,p) \leq 1$. Donc,

  $$\Lambda_2 \leq \prod_{p \in \mathcal{P},\, \sqrt{2n} < p \leq \frac{2n}{3}} p \leq \exp\left(\theta\left(\frac{2n}{3} \right) \right) < 4^{\frac{2n}{3}}$$

  par le lemme de majoration de θ.
- Reste à majorer Λ_3. En fait il s'agit de voir que si $\frac{2n}{3} < p \leq n$ avec $p \in \mathcal{P}$, alors $\beta(n,p) = 0$. En effet, on a alors

  $$\beta(n,p) = \left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor = 2 - 2 = 0.$$

  De cette remarque on tire $\Lambda_3 = 1$.

On dispose de tout ce qu'il faut pour conclure. On a donc

$$\frac{4^n}{2n} \leq \Lambda_1 \Lambda_2 \Lambda_3 \Lambda_4$$

ce qui donne avec les majorations précédentes,

$$\Lambda_4 > \frac{4^{\frac{n}{3}}}{(2n)^{\sqrt{2n}+1}}.$$

On en tire,

$$\ln(\Lambda_4) > \frac{n}{3} \ln(4) - (\sqrt{2n} + 1) \ln(2n).$$

On vérifie que pour tout $n \geq 631$ le terme de droite est strictement positif ce qui donne le résultat voulu.

Preuve du théorème de Tchebychev pour $2 \leq n \leq 630$. La technique qui suit permet de facilement démontrer le théorème de Tchebychev pour les "petits" nombres. Il s'agit du procédé de Landau. L'idée est de commencer par établir la liste de onze nombres premiers suivante

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$$

choisie de sorte à ce que chaque nombre premier de cette liste soit strictement inférieur au double du nombre qui le précède. Fixons maintenant un entier n dans $\{2, \ldots, 630\}$. On peut trouver deux nombres premiers consécutifs q et p dans la liste qui précède tels que $q \leq n < p$. Alors, on a aussi $2q > p$ et $2q \leq 2n$, ce qui impose

$$q \leq n < p < 2q \leq 2n$$

et en particulier

$$n < p < 2n$$

ce qui est bien le résultat recherché.

3 Compléments sur le postulat de Bertrand

3.1 La conjecture de Legendre

Le postulat de Bertrand étant à présent démontré, il est d'usage de laisser parler le mathématicien qui sommeille en chacun de nous et de se poser une simple question : ne peut-on pas améliorer ce résultat ? La réponse n'est en fait absolument pas claire ! Par exemple, il existe (voir ci-après) des conjectures très similaires au postulat de Bertrand qui restent néanmoins aujourd'hui encore sans réponse.

Conjecture de Legendre. *Soit $n \geq 1$ un entier, alors il existe un nombre premier p vérifiant*

$$n^2 < p < (n+1)^2.$$

3.2 La preuve historique de Tchebychev

On donne ici la preuve historique du postulat de Bertrand. Introduisons déjà quelques notations. Si $x \in \mathbb{R}$, on note

$$\pi(x) = |\{p \in \mathcal{P}\ ,\ p \leq x\}|\,.$$

$\pi(x)$ évalue donc pour $x \in \mathbb{R}$ le nombre de nombres premiers inférieurs à x. Le postulat de Bertrand se ramène donc à établir que pour tout $n \geq 2$ entier,

$$\pi(2n) - \pi(n) > 0.$$

Tchebychev est parvenu à montrer ceci pour n suffisamment grand. Il a en effet obtenu l'existence de $\alpha \sim 0,92$, $\beta \sim 1,1$ et $n_0 \in \mathbb{N}^*$ tels que pour tout $n \geq n_0$,

$$\alpha \frac{n}{\ln(n)} < \pi(n) < \beta \frac{n}{\ln(n)}.$$

Avec un tel encadrement, il a pu minorer la quantité $\pi(2n) - \pi(n)$ et obtenir le résultat recherché. Il n'a cependant jamais réussi à évaluer avec "suffisamment de précision" la quantité $\pi(n)$ pour obtenir ce qui porte aujourd'hui le nom de théorème des nombres premiers (voir section suivante).

4 Annexe : Répartition des nombres premiers

4.1 Le théorème des nombres premiers.

C'est le mathématicien Johann Carl Friedrich Gauss qui a énoncé le premier les conjectures les plus précises pour ce qui concerne l'évaluation asymptotique de $\pi(x)$: il conjecture ainsi

$$\pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\ln(x)}$$

ce qui signifie que $\pi(x)$ est à "peu près égal" à $\frac{x}{\ln(x)}$ pour des réels x suffisamment grands. Cette remarquable conjecture effectuée en 1792 résistera à de nombreux mathématiciens et notamment à Tchebychev qui parviendra tout de même à montrer le résultat suivant :

Théorème de Tchebychev (1821). *Si jamais il existe $c > 0$ tel que*

$$\pi(x) \underset{x\to+\infty}{\sim} c\frac{x}{\ln(x)}$$

alors $c = 1$.

Ce résultat ainsi que l'encadrement présenté dans la section précédentes constituaient déjà de grandes avancées. Il faudra finalement attendre l'année 1896 pour que les mathématiciens Jacques Hadamard (Français) et Charles de La Vallée-Poussin (Belge) démontrent indépendamment mais de la même manière ce qui porte désormais le nom de théorème des nombres premiers.

Théorème des nombres premiers (1896). *On a l'estimation suivante,*

$$\pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\ln(x)}.$$

4.2 Quelques conjectures célèbres

On énoncé ici certaines conjectures mathématiques célèbres en théorie des nombres et qui, pour certaines, résistent au mathématicien depuis plus de 200 ans !

Conjecture des nombres premiers jumeaux. *Il existe une infinité de couples (p, q) de nombres premiers vérifiant $|p - q| = 2$.*

Conjecture de Goldbach (1742). *Tout entier pair $n \geq 3$ peut s'écrire comme somme de deux nombres premiers.*

Conjecture de Goldbach faible. *Tout entier impair $n \geq 9$ peut s'écrire comme somme de trois nombres premiers*[3].

On termine en mentionnant le lien entre les nombres premiers et la célèbre conjecture de Riemann.

3. Une preuve, toujours en vérification, a été proposé en 2013 par un mathématicien Péruvien : Harald Helfgott.

4.3 La conjecture de Riemann

Commençons par introduire la célèbre fonction ζ de Riemann que l'on peut définir sur le demi-plan $\mathbb{D} = \{z \in \mathbb{C}\,,\, \Re(z) > 1\}$ par,

$$\zeta(z) = \sum_{n=1}^{+\infty} \frac{1}{n^z}.$$

La fonction ζ se prolonge en fait sur $\mathbb{C} \setminus \{1\}$. L'introduction de cette fonction remonte à l'immense mathématicien suisse Leonhard Euler (1707-1783) qui montrera notamment les formules suivantes :

$$\zeta(2) = \sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

et pour $s \in]1, +\infty[$,

$$\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}.$$

Apparaît alors par cette seconde formule un lien entre ζ et les nombres premiers qui n'a cessé d'étonner les mathématiciens. La fonction ζ contient une information essentielle sur la répartition des nombres premiers : par exemple, le théorème des nombres premiers équivaut en fait à la non-annulation de ζ sur la droite $\{z \in \mathbb{C}\,,\, \Re(z) = 1\}$. Mieux encore, en 1859 le mathématicien allemand Bernhard Riemann émet l'hypothèse suivante

Conjecture de Riemann (1859). *Les zéros non triviaux*[4] *de la fonction ζ sont localisés sur la droite $\left\{z \in \mathbb{C}\,,\, \Re(z) = \frac{1}{2}\right\}$.*

Si cette hypothèse s'avérait être vraie, on obtiendrait une estimation remarquable de la fonction π introduite dans la section précédente. Plus formellement, on peut montrer que la conjecture de Riemann est équivalente à la proposition suivante

Formulation équivalente de la conjecture de Riemann (Schoenfeld, 1976). *Notons pour $x > 0$, $\mathrm{Li}(x) = \int_0^x \frac{dt}{\ln(t)}$ (le logarithme intégrale). Alors, pour $x \geq 2657$,*

$$|\pi(x) - \mathrm{Li}(x)| \leq \frac{1}{8\pi}\sqrt{x}\log(x).$$

De nombreuses preuves de la conjecture de Riemann ont déjà été proposées mais à ce jour aucune de ces preuves n'a pu être validée. Pour de nombreux mathématiciens il s'agit du problème ouvert actuel le plus beau, notamment du fait de l'impressionnante multiplicité de ses formulations équivalentes. Il s'agit enfin d'un problème mis à prix par l'institut Clay en 2000, mais sa résolution apporterait bien plus que le million de dollar promis à quiconque apporterait une solution valide... À vous de jouer !

4. La fonction ζ admet un certain nombre de zéros dits *triviaux* qui sont localisés en les entiers de la forme $-2k$ où $k > 0$. Ces zéros étant parfaitement connus des mathématiciens depuis longtemps déjà, il s'agit à présent de trouver les zéros non triviaux : c'est l'objet de la conjecture de Riemann.

5 Compléments : lemmes calculatoires

Propriétés du coefficient binomial. *On a les propriétés suivantes :*

(*i*) *Pour tout* $n, k \in \mathbb{N}$, $\binom{n}{k}$ *est un entier.*

(*ii*) *Pour tout* $n \geq 0$, $\binom{n}{0} = \binom{n}{n} = 1$.

(*iii*) *Pour tout* $0 \leq k \leq n$, $\binom{n}{k} = \binom{n}{n-k}$.

(*iv*) *Si* $n \in \mathbb{N}$, *la suite* $\left(\binom{n}{k}\right)_{k \geq 0}$ *est croissante jusqu'à* $k = \lfloor \frac{n}{2} \rfloor$ *puis décroît. En particulier, il faut retenir que pour tout* $k \in \mathbb{N}$,

$$\binom{n}{k} \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

(*v*) *Si* $n \geq 0$,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

(*vi*) *On dispose de la formule de Pascal : si* $n, k \in \mathbb{N}$, *alors*

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

(*vii*) *Si* $n, k \in \mathbb{N}^*$,

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

On commence par démontrer les 6 derniers points et on conclut sur le premier point par une récurrence astucieuse.

(*ii*) Il suffit de revenir à la définition du coefficient binomial en utilisant le fait que $0! = 1$.

(*iii*) Si $n \geq 0$ et $k \in \{0, \ldots, n\}$,

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

(*iv*) Soit $n \in \mathbb{N}^*$ (le résultat est clair si $n = 0$). Soit $k \in \{1, \ldots, n\}$. On remarque que

$$\binom{n}{k-1} \leq \binom{n}{k} \Leftrightarrow k!(n-k)! \leq (k-1)!(n-k+1)! \Leftrightarrow k \leq (n-k+1) \Leftrightarrow k \leq \frac{n+1}{2}.$$

Comme k est entier ceci équivaut à

$$k \leq \left\lfloor \frac{n+1}{2} \right\rfloor.$$

Ceci permet de montrer que la suite des coefficients binomiaux est strictement croissante sur $0 \leq k \leq n/2$ puis strictement décroissante sur $n/2 \leq k \leq n$.

(*v*) On utilise la formule du binôme de Newton démontré après :

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k}.$$

(*vi*) On commence par vérifier la formule si $0 \leq k \leq n-1$. On a alors,

$$\binom{n}{k} + \binom{n}{k+1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} = \frac{n!(k+1)!(n-k-1)! + n!k!(n-k)!}{k!(n-k)!(k+1)!(n-k-1)!}$$

$$= \frac{n!(k+1) + n!(n-k)}{(k+1)!(n-k)!} = \frac{(n+1)!}{(k+1)!(n-k)!} = \binom{n+1}{k+1}.$$

Si maintenant $k = n$, on a

$$\binom{n}{n} + \binom{n}{n+1} = 1 + 0 = \binom{n+1}{n+1}.$$

On vérifie enfin que la formule est vraie si $k > n$.

(*vii*) Observons que si $1 \leq n < k$, la formule est vraie. Supposons donc $1 \leq k \leq n$. On a

$$\frac{n}{k}\binom{n-1}{k-1} = \frac{n(n-1)!}{k(k-1)!(n-k)!} = \binom{n}{k}.$$

(*i*) Le résultat s'obtient par récurrence sur n avec la formule de Pascal. Ceci s'observe sur le schéma suivant (triangle de Pascal), où chaque coefficient binomial est la somme des deux coefficients binomiaux qui se trouvent au dessus. Comme l'on sait que pour tout $n \in \mathbb{N}$, $\binom{n}{0} = \binom{n}{n} = 1 \in \mathbb{N}$, la formule de Pascal suffit effectivement à conclure. Une autre méthode consisterait à connaitre l'interprétation combinatoire du coefficient binomial $\binom{n}{k}$: il s'agit en fait du nombre de manières de choisir k éléments dans un ensemble de n éléments.

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$

Binôme de Newton. *Si $a, b \in \mathbb{R}$ et $n \geq 0$, alors*

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

Démontrons ce résultat par récurrence sur $n \geq 0$. La preuve qui suit utilise la propriété (*vi*) du point précédent. Si $n \geq 0$,

HR_n : " Pour tout $a, b \in \mathbb{R}$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ ".

HR_0 est clairement vraie. Supposons $n \geq 1$ et HR_{n-1} vraie. On écrit, si $a, b \in \mathbb{R}$,

$$(a+b)^n = (a+b)^{n-1}(a+b) \underset{\mathrm{HR}_{n-1}}{=} \left(\sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{(n-1)-k} \right) (a+b)$$

$$= \sum_{k=0}^{n-1} \binom{n-1}{k} a^{k+1} b^{(n-1)-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-k} = \sum_{k=1}^{n} \binom{n-1}{k-1} a^k b^{n-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-k}$$

$$= \sum_{k=1}^{n-1} \left(\binom{n-1}{k-1} + \binom{n-1}{k} \right) a^k b^{n-k} + a^n b^0 + a^0 b^n \underset{(vi)}{=} \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

D'où HR_n.

6 Exercices

Exercice 5 (*Nombres de Fermat*).

1) Déterminer une condition nécessaire sur $m \in \mathbb{N}$ pour que le nombre $2^m + 1$ soit premier

On pose pour $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$: c'est le n-ième nombre de Fermat.

2) Vérifier que F_0, F_1, F_2, F_3 et F_4 sont des nombres premiers. F_5 est-il premier ? (On remarquera que $641 = 5^4 + 2^4 = 1 + 5.2^7$).
3) Prouver que si $n \neq m$ alors $F_n \wedge F_m = 1$. Retrouver le théorème d'Euclide (c'est à dire le fait qu'il existe une infinité de nombres premiers).

Exercice 6. Soit $k \geq 2$. Montrer que le produit de trois entiers naturels non nuls consécutifs ne peut pas être une puissance k-ième.

Exercice 7 (*Minoration de Tchebychev*). On note $\mathcal{P}$ l'ensemble des nombres premiers. On note $\pi(x)$ le nombre de nombres premiers (positifs) au plus égaux à x.

1) Montrer la formule de Legendre.
2) Montrer que
$$\binom{2n}{n} \text{ divise } \prod_{p\in\mathcal{P},\, p\leq 2n} p^{\lfloor \frac{\ln(2n)}{\ln(p)} \rfloor}.$$
3) Montrer que
$$\binom{2n}{n} \leq (2n)^{\pi(2n)}.$$
4) En déduire qu'il existe $C > 0$ telle que pour tout $n \geq 2$,
$$C\frac{n}{\ln n} \leq \pi(n).$$

Exercice 8. Justifier l'existence de 1000 entiers consécutifs sans nombres premiers.

Exercice 9 (*Nombres de Mersenne*). On suppose que $n \geq 2$ est tel que $2^n - 1$ est premier. Montrer que n est un nombre premier.

Exercice 10 (*Un exercice pour Gauss*). Soient $n \geq \mathbb{N}^*$, k un entier impair, montrer que
$$1 + \ldots + n \mid 1^k + \ldots + n^k.$$

Exercice 11.

1) Montrer que l'ensemble des nombres premiers est infini.
2) Pour $n \in \mathbb{N} \setminus \{0, 1\}$, on note $p(n)$ le plus grand diviseur premier de n et on pose $E = \{n \geq 2\,,\, p(n) < p(n+1) < p(n+2)\}$. Soit q un nombre premier différent de 2. Pour $n \geq 1$, on pose $u_n = q^{2^n} - 1$ et $v_n = q^{2^n} + 1$. Montrer que $(u_n \notin E) \Leftrightarrow (\, p(u_n) \geq q$ ou $p(v_n) \leq q\,)$.
3) Montrer que si $(m, n) \in \mathbb{N}^2$ avec $m \neq n$, alors
$$\left(\frac{v_n}{2}\right) \wedge \left(\frac{v_m}{2}\right) = 1.$$
4) En déduire que E est infini.

7 Correction des exercices

Solution exercice 2. *Notons $X = \{p \in \mathcal{P}\ ,\ p \equiv 3[4]\}$. Montrons que X est infini. On raisonne par l'absurde en supposant X fini et on note $X = \{p_1, \dots, p_n\}$. Posons*

$$\alpha = 4p_1 \dots p_n - 1.$$

Observons que $\alpha \equiv 3[4]$ et $\alpha > 1$. De plus, α admet un diviseur premier, comme α est impair ce diviseur premier ne peut être 2 et par construction un tel diviseur ne peut être congru à 3 modulo 4 : il est donc congru à 1 modulo 4 et c'est le cas de tous les diviseurs premiers de α. On en déduit en décomposant α comme produit de facteurs premiers que $\alpha \equiv 1[4]$ et cela est en contradiction avec ce qui précède.

Solution exercice 3. *On commence par écrire*

$$\binom{p^n}{k} = \frac{p^n(p^n-1)\dots(p^n-k+1)}{k!}.$$

On remarque ensuite que si $i \in [\![1, k-1]\!]$ alors $v_p(p^n - i) = v_p(i)$. Alors, on en déduit

$$v_p\left(\binom{p^n}{k}\right) = v_p\left(p^n(p^n-1)\dots(p^n-k+1)\right) - v_p(k!) = v_p(p^n) + \sum_{i=1}^{k-1} v_p(p^n-i) - \sum_{i=1}^{n} v_p(i) = n - v_p(k).$$

Solution exercice 5.

1) *On montre que si $m \in \mathbb{N}$ est tel que $2^m + 1 \in \mathcal{P}$, alors m est une puissance de 2. En effet, on peut écrire si $m \geq 1$, $m = 2^\alpha\beta$ où β est impair. Montrons que sous l'hypothèse que $2^m + 1$ est premier on doit avoir $\beta = 1$. On écrit*

$$2^m + 1 = (2^{2^\alpha})^\beta - (-1)^\beta = (2^\alpha + 1)\sum_{k=0}^{\beta-1}(2^\alpha)^k(-1)^{\beta-1-k}.$$

En particulier $2^\alpha + 1$ divise le nombre premier $2^m + 1$, c'est que nécessairement $2^\alpha = m$.

2) *On a $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ sont des nombres premiers (facile de s'en convaincre pour F_3 et on l'admet pour F_4). Ensuite montrons que F_5 n'est pas premier. On écrit $5.2^7 \equiv -1[641]$ et en élevant à la puissance 4, $5^4 2^{28} \equiv 1[641]$. Or $5^4 \equiv -2^4[641]$ d'où $2^{32} + 1 \equiv F_5 \equiv 0[641]$ et 641 divise F_5 qui n'est donc pas premier.*

3) *On choisit donc $n < m$ deux entiers. On a $F_m = (2^{2^n})^{2^{m-n}} + 1 = (F_n - 1)^{2^{m-n}} + 1$. On réduit modulo F_n et on obtient,*

$$F_m \equiv 2[F_n].$$

Si jamais F_n et F_m admettaient un diviseur commun autre que 1 ce serait forcément 2 : or ceci est impossible car F_n et F_m sont impairs. On a donc obtenu $F_n \wedge F_m = 1$.
Supposons à présent par l'absurde $\mathcal{P}$ fini. Comme la suite $(F_n)_{n\in\mathbb{N}}$ est constituée d'entiers premiers entre eux deux à deux et que chacun de ces entiers admet un diviseur premier on aboutit nécessairement à une absurdité. Autrement dit, on peut injecter $\mathbb{N}$ dans $\mathcal{P}$ via l'application qui à un nombre de Fermat associe n'importe lequel de ses diviseurs premiers. Il en découle que $\mathcal{P}$ est nécessairement infini.

Solution exercice 6. *On raisonne par l'absurde en supposant l'existence de deux entiers $n \geq 2$ et $a \geq 1$ tels que*

$$a^k = (n-1)n(n+1).$$

On a donc $a^k = (n^2-1)n$. Observons déjà que

$$n^2 - 1 \wedge n = 1.$$

En effet, ceci provient du théorème de Bézout et de la relation $n \times n - 1 \times (n^2-1) = 1$. On observe alors le résultat suivant :

Lemme : *Soient α et β deux entiers ≥ 1 et premiers entre eux tels que $\alpha\beta$ soit une puissance k-ième. Alors α et β sont des puissances k-ièmes.*

Preuve du lemme : *Écrivons $\alpha\beta = \gamma^k$ et la décomposition en facteurs premiers de γ :*

$$\gamma = \prod_{i=1}^{r} p_i^{\alpha_i}.$$

Avec cette écriture on voit que les facteurs premiers de α et β sont exactement parmi les p_i et comme α et β sont premiers entre eux on peut trouver deux parties I et J de $\{1, \ldots, r\}$ disjointes non vides telles que :

- *$I \sqcup J = \{1, \ldots, r\}$.*
- *$\alpha = \prod_{i \in I} p_i^{\alpha_i k}$ et $\beta = \prod_{j \in J} p_i^{\alpha_j k}$.*

On en déduit

$$\alpha = \left(\prod_{i \in I} p_i^{\alpha_i} \right)^k \text{ et } \beta = \left(\prod_{j \in J} p_i^{\alpha_j} \right)^k.$$

D'où le lemme.

On en revient à notre énoncé. On applique ce lemme à n et $n^2 - 1$ et on a deux entiers y et z tels que $n = y^k$ et $n^2 - 1 = z^k$. Alors

$$y^{2k} - z^k = 1.$$

On en tire $y^2 > z$. Or par hypothèse $z > 1$ (sans quoi $n = 1$) donc,

$$y^{2k} - z^k \geq (z+1)^k - z^k \geq k > 1.$$

Ceci fournit la contradiction recherchée.

Solution exercice 7.

1) *Voir proposition 2.16.*
2) *D'après la formule de Legendre, si $p \in \mathcal{P}$,*

$$v_p\left(\binom{2n}{n}\right) = \sum_{k=1}^{+\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

Comme pour $x \in \mathbb{R}$, $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\}$, les termes de cette sommes sont nuls ou égaux à 1 et en particulier,

$$v_p\left(\binom{2n}{n}\right) \leq \left| \left\{ k \in \mathbb{N}^*, \ \left\lfloor \frac{2n}{p^k} \right\rfloor > 0 \right\} \right| = \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor.$$

On en déduit le résultat voulu.

3) *Il suffit d'écrire que si* $p \in \mathcal{P}$, *alors* $\left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor \leq \frac{\ln(2n)}{\ln(p)}$. *Ainsi, comme si* $a, b \geq 1$ *sont tels que* a *divise* b *alors* $a \leq b$, *on en déduit*

$$\binom{2n}{n} \leq \prod_{p\in\mathcal{P},\, p\leq 2n} p^{\lfloor \frac{\ln(2n)}{\ln(p)} \rfloor} \leq \prod_{p\in\mathcal{P},\, p\leq 2n} p^{\frac{\ln(2n)}{\ln(p)}} = (2n)^{\pi(2n)}.$$

4) *On passe au* ln *dans l'inégalité précédente et on obtient pour* $n \geq 1$,

$$\sum_{k=1}^{2n} \ln(k) - 2\sum_{k=1}^{n} \ln(k) \leq \ln(2n)\pi(2n).$$

Or une comparaison série intégrale[5] *permet d'évaluer le terme de gauche et de voir que*

$$\sum_{k=1}^{2n} \ln(k) - 2\sum_{k=1}^{n} \ln(k) \underset{n\to+\infty}{\sim} \ln(2)(2n).$$

Ainsi,

$$\frac{2n}{\ln(2n)} \underset{n\to+\infty}{=} \mathcal{O}(\pi(2n)).$$

Il suffit alors de voir que $\pi(2\lfloor x/2 \rfloor) \underset{x\to+\infty}{\sim} \pi(x)$ *et*

$$\frac{2\lfloor x/2 \rfloor}{\ln(2\lfloor x/2 \rfloor)} \underset{x\to+\infty}{\sim} \frac{x}{\ln(x)}$$

pour conclure sur l'existence de la constante $C > 0$ *souhaitée.*

Solution exercice 8. *Prenons par exemple* $\{1001! + i\ ,\ i \in [\![2, 1001]\!]\}$. *On voit en particulier qu'on peut trouver des suites d'entiers consécutifs sans nombres premiers arbitrairement grandes.*

Solution exercice 9. *Écrivons* $n = ab$ *où* $a, b \geq 1$ *sont deux entiers. Montrons que nécessairement* a *ou* b *est égal à* 1. *On écrit,*

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)\sum_{k=0}^{b-1} (2^a)^k.$$

Et en particulier $2^a - 1$ *divise* $2^n - 1$ *qui est premier par hypothèse, donc* $2^a - 1 \in \{1, 2^n - 1\}$ *et* $a \in \{1, n\}$, *d'où le résultat.*

Bibliographie

[E] P.Erdös. Beweis eines Satzes von Tschebyschef . Acta.Litt.Sci.Szeged 5,194-198 (1932).

[HW] G. H. Hardy & E. M. Wright, « An Introduction to the Theory of Numbers » (1re éd. 1938), 4e éd., p. 341-344.

[R] S. Ramanujan, « A proof of Bertrand's postulate », Journal of the Indian Mathematical Society, XI, 1919, p. 181-182.

5. Pour comprendre ce passage, il vous faudra sans doute patienter jusqu'au chapitre "Séries numériques" de votre première année de classe préparatoire.