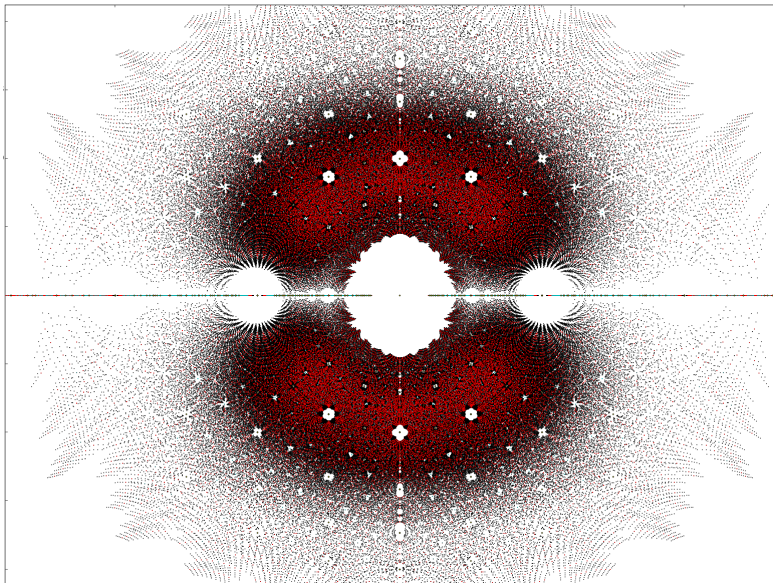
Rapport de stage de M1 :

Sur une preuve de la conjecture de Schinzel-Zassenhaus, d'après Dimitrov

Léo Dubocs
encadré par Fabien Pazuki

Juillet 2022



Département de Mathématiques et Applications
École Normale Supérieure

Table des matières

Déroulement du stage

J'ai effectué mon stage de M1 de mars à juin en théorie des nombres à l'université de Copenhague, sous la direction de Fabien Pazuki. Le but de ce stage était de comprendre la preuve récente de la conjecture de Schinzel-Zassenhaus, prouvée fin 2019 par Dimitrov dans [SZ65]. Cette preuve utilise des outils que je n'avais peu ou pas eu l'occasion de manipuler, tels que le diamètre transfini, les nombres p-adiques ou encore les fonctions harmoniques. Cela a donc été pour moi l'occasion de découvrir ces notions et d'avoir un aperçu de ce qu'est la recherche en mathématiques.

Lors de ce stage, en plus de mon travail de compréhension d'articles, j'ai suivi un cours d'introduction à la théorie algébrique des nombres. J'ai également assisté aux séminaires de l'équipe de théorie des nombres, ainsi que de manière plus occasionnelle aux séminaires d'autres équipes. Mon stage s'est conclu par un exposé d'une heure que j'ai donné dans le cadre du séminaire de théorie des nombres.

En avril, j'ai eu la chance de pouvoir assister au *Crafoord Prize Symposium in Number Theory* à Lund (Suède), en l'honneur d'Enrico Bombieri. J'ai ainsi pu assister à des conférences par des chercheurs de renommée internationale en théorie des nombres, dont James Maynard (lauréat médaille Fields 2022).

Sur le plan plus personnel, j'ai réussi à trouver un groupe de musique dans lequel jouer, et nous avons participé au *DIKU Revy* : tradition du département d'informatique datant d'une cinquantaine d'années, il s'agit d'un spectacle entièrement organisé par des étudiants alliant musique et sketchs. J'ai également profité de ce séjour pour faire un peu de vélo lors des allers-retours à l'université, et bien évidemment pour visiter cette ville magnifique qu'est Copenhague.

Je tiens à remercier chaleureusement toute l'équipe de théorie des nombres de l'université de Copenhague, et en particulier mon maître de stage Fabien Pazuki, pour ce stage qui m'a énormément plu. Je remercie également mon tuteur à l'ENS Farrell Brumley qui m'a permis de trouver ce stage.

Introduction mathématique

Fixons $P = \prod(X - \alpha_i) \in \mathbb{Z}[X]$ un polynôme unitaire, irréductible et à coefficients entiers. On note n son degré, on suppose $n \geq 2$ et que P n'est pas un polynôme cyclotomique.

En 1857, Kronecker prouve :

$$\max |\alpha_i| > 1.$$

En 1965, Schinzel et Zassenhaus cherchent à améliorer ce résultat. Ils prouvent dans [SZ65] :

$$\max |\alpha_i| \geq 1 + \frac{1}{16} 2^{-n}$$

Ils notent que la constante $1/16$ pourrait sûrement être améliorée, mais que l'intérêt est limité puisque l'ordre de grandeur de $(\max |\alpha_i| - 1)$ devrait être beaucoup plus gros que la décroissance exponentielle prouvée. Ils ajoutent :

« In fact, we cannot disprove $\max |\alpha_i| > 1 + \frac{c}{n}$, where $c > 0$ is an absolute constant. »

Cette question a par la suite été appelée la conjecture de Schinzel-Zassenhaus.

Au fil des années, divers résultats partiels ont été obtenus sur cette conjecture, on en cite ici deux :

— En 1971, Smyth [Smy71] prouve que si P n'est pas un polynôme réciproque (ou palindromique), alors la conjecture de Schinzel-Zassenhaus est vraie, avec une constante explicite qu'il exhibe.

— En 1979, Dobrowolski [Dob79] prouve que pour tout $\varepsilon > 0$, si P est un polynôme réciproque et si son degré n est assez grand, alors :

$$\max |\alpha_i| \geq 1 + \frac{2 - \varepsilon}{n} \left(\frac{\log \log n}{\log n} \right)^3$$

ce qui se rapproche sensiblement de la borne attendue par la conjecture, mais n'est valable qu'asymptotiquement.

Finalement, en 2019, Dimitrov démontre dans [Dim19] le résultat suivant, qui prouve la conjecture de Schinzel-Zassenhaus :

Théorème 1. *Soit $P = \prod_{i=1}^{n} (X - \alpha_i) \in \mathbb{Z}[X]$ un polynôme à coefficients entiers, unitaire et irréductible. On suppose que $n \geq 2$ et que P n'est pas un polynôme cyclotomique. Alors*

$$\max |\alpha_i| \geq 2^{\frac{1}{4n}} \geq 1 + \frac{\log 2}{4n}.$$

Le but de ce mémoire est de s'intéresser aux outils utilisés dans la preuve de Dimitrov, notamment la notion de diamètre transfini qui y joue un rôle central. Sa preuve de la conjecture est ensuite donnée, et on termine par quelques idées en vue d'une généralisation.

1 Diamètre transfini

Le diamètre transfini est une notion qui permet de mesurer la taille d'un compact. Il joue un rôle crucial dans la preuve par Dimitrov de la conjecture de Schinzel-Zassenhaus.

1.1 Définition et premières propriétés

Définition 1. Soit $E \subseteq \mathbb{C}$ un compact non vide. On définit :

$$d_n = \left(\max_{z_1,\dots,z_n \in E} \prod_{1 \leq i < j \leq n} |z_i - z_j| \right)^{\frac{2}{n(n-1)}}.$$

Remarque. Remarquons que le maximum est atteint, par compacité de E.

Remarque. d_2 correspond à la notion usuelle de diamètre d'un ensemble compact. Dans le cas général, la puissance $\frac{2}{n(n-1)}$ correspond à une moyenne géométrique des distances mises en jeu. En termes physiques, elle assure que d_n a la dimension d'une longueur.

On montre que la suite (d_n) est décroissante, voir par exemple [Hay65]. Cela nous amène à la définition suivante :

Définition 2. Le *diamètre transfini* de E est la limite $d(E) = \lim_{n\to\infty} d_n$.

Avec cette définition, on obtient de manière immédiate :

Proposition 1. *Soient $E, F \subseteq \mathbb{C}$ des compacts, et soit $a \in \mathbb{C}$. On a :*

1. $d(E) \geq 0$.
2. $d(E) \leq d_2(E)$.
3. *Si $E \subseteq F$, alors* $d(E) \leq d(F)$.
4. $d(a + E) = d(E)$, *où* $a + E = \{a + x \mid x \in E\}$.
5. $d(aE) = |a|\, d(E)$, *où* $aE = \{ax \mid x \in E\}$.

Exemple.

— Si E est un ensemble fini, $d(E) = 0$.

— Si $E = C(0, 1)$ est le cercle unité, on pourrait calculer le diamètre transfini de la manière suivante : on choisit n points sur le cercle $e^{i\theta_1}, \dots, e^{i\theta_n}$, et on voit $\prod_{1 \leq k < l \leq n} |e^{i\theta_k} - e^{i\theta_l}|$ comme une fonction des θ_j, que l'on cherche à minimiser en différenciant... mais cette approche est extrêmement longue et fastidieuse !

La définition de d rend fastidieuse toute tentative de calculer le diamètre transfini d'un compact donné, même les plus simples. Nous avons besoin de regarder le problème d'un autre angle.

1.2 La constante de Tchebychev

Définition 3. Soit $E \subseteq \mathbb{C}$ un compact. On dénote par $\mathcal{P}_n$ l'ensemble des polynômes unitaires $P \in \mathbb{C}[X]$ de degré n. On définit

$$m_n = \min_{P \in \mathcal{P}_n} \max_{z \in E} |P(z)|.$$

A nouveau, le maximum est atteint par compacité de E, on montre que le minimum est lui aussi atteint.

Définition 4. Les polynômes qui atteignent le minimum dans la définition de m_n sont appelés *polynôme de Tchebychev* de degré n. On désigne un de ces polynômes par t_n.

Remarque. Dans le cas du segment $[-1, 1]$, t_n est unique et vaut $t_n = T_n/2^{n-1}$, où T_n est le polynôme de Tchebychev usuel, *ie* satisfaisant $T_n(\cos\theta) = \cos(n\theta)$. Ceci explique la terminologie choisie pour les polynômes t_n.

En suivant [Gol69], on montre que la suite $(m_n^{1/n})$ converge.

Définition 5. On appelle *constante de Tchebychev* la limite $\tau(E) = \lim_{n\to\infty} m_n^{1/n}$.

Théorème 2. *Pour tout compact E, $d(E) = \tau(E)$.*

Idée de démonstration. On note $V_n = d_n^{n(n-1)/2}$. Grâce à des manipulations algébriques, et en remarquant que la définition de V_n fait intervenir un déterminant de Vandermonde, on prouve $m_n \leq \dfrac{V_{n+1}}{V_n} \leq (n+1)m_n$. Puis on multiplie ces relations ensemble pour $n = 2, 3, \ldots, N$, on prend la puissance $\frac{2}{N(N+1)}$ et enfin la limite $N \to \infty$.

La preuve est détaillée dans [Gol69]. □

1.3 Calculs explicites de diamètre transfini

Cette correspondance agréable entre diamètre transfini et constante de Tchebychev nous permet de calculer bien plus facilement le diamètre transfini de certains compacts.

Proposition 2.

1. *Soit $C(0, R)$ le cercle de centre 0 et de rayon R. Alors $d(C(0, R)) = R$.*
2. *Soit $[0, b]$ un segment de droite. Alors $d([0, b]) = b/4$.*

Démonstration. Les deux preuves pour le cercle et le segment sont similaires, tirées de [Gol69]. On ne prouve ici que le cas du cercle.

Soit $p_n(z) = z^n + c_{n-1}z^{n-1} + \cdots + c_0$ un polynôme unitaire arbitraire de degré n. En écrivant $z = Re^{i\theta}$, on a

$$\begin{aligned}
\max_{z\in C(0,R)} |p_n(z)|^2 &\geq \frac{1}{2\pi}\int_0^{2\pi} |p_n(z)|^2 \,\mathrm{d}\theta \\
&= \frac{1}{2\pi}\int_0^{2\pi} p_n(z)\overline{p_n(z)} \,\mathrm{d}\theta \\
&= \frac{1}{2\pi}\int_0^{2\pi} (R^n e^{in\theta} + c_{n-1}R^{n-1}e^{i(n-1)\theta} + \cdots + c_0)\,. \\
&\qquad\qquad (R^n e^{-in\theta} + \overline{c_{n-1}}R^{n-1}e^{-i(n-1)\theta} + \cdots + \overline{c_0}) \,\mathrm{d}\theta \\
&= R^{2n} + |c_{n-1}|^2 R^{2(n-1)} + \cdots + |c_0|^2 \\
&\geq R^{2n}
\end{aligned}$$

Donc $m_n \geq R^n$. Mais pour $p_n(z) = z^n$, $\max_{z\in C(0,R)} |p_n(z)| = R^n$. Par conséquent $m_n = R^n$ and $\tau(C(0,R)) = R$. □

On donne encore deux propositions, assorties d'exemples, qui permettent d'augmenter largement le nombre de compacts dont on sait calculer explicitement le diamètre transfini.

Proposition 3. *Soit E un compact, et notons ∂E sa frontière. Alors*

$$d(E) = d(\partial E).$$

Démonstration. La proposition est conséquence du principe du maximum. □

Exemple. Grâce aux propositions 2 et 3, on obtient $d(\bar{B}(0,R)) = R$, où $\bar{B}(0,R)$ est la sphère fermée de centre 0 et de rayon R.

Proposition 4. *Soit E un compact et soit $P \in \mathcal{P}_n$. Alors*

$$d(P^{-1}(E)) = d(E)^{1/n}.$$

Exemple. Soit $E = \bigcup_{k=1}^{n}[0, e^{2ik\pi/n}]$ une "étoile" régulière à n branches. Alors E est l'image inverse du segment $[0,1]$ par le polynôme $P(z) = z^n$. En utilisant les propositions 2 et 4, il vient : $d(E) = d([0,1])^{1/n} = \dfrac{1}{4^{1/n}}$.

2 Capacité et théorème de Dubinin

Le changement de point de vue entre diamètre transfini et constante de Tchebychev nous a permis de gagner beaucoup d'informations sur cette notion. On a ici la chance de disposer d'un troisième point de vue à explorer !

2.1 Capacité

Définition 6. Soit $B \subseteq \mathbb{C}$ un ouvert connexe, voisinage de l'infini. On dit que $g : \mathbb{C} \to \mathbb{R}$ est la *fonction de Green* de B si :

1. g est harmonique sur B
2. $g = 0$ sur $\mathbb{C} \setminus B$
3. Il existe une constante $\gamma \in \mathbb{R}$ telle que $g(z) = \log|z| + \gamma + o(1)$ quand $z \to \infty$.

La constante γ est appelée *constante de Robin*.

Remarque. La fonction de Green, si elle existe, est unique. En effet, si deux telles fonctions existent, leur différence est harmonique, bornée, et prend pour valeur 0 sur $\mathbb{C} \setminus B$. D'après le théorème de Liouville, cette différence est donc nulle.

Définition 7. Soit E un compact de $\mathbb{C}$, et soit B la composante connexe du complémentaire de E qui est un voisinage de l'infini.

Si la fonction de Green de B existe, on définit la *capacité* de E comme étant $\mathrm{cap}(E) = e^{-\gamma}$, où γ est la constante de Robin.

Si B n'admet pas de fonction de Green, on définit $\mathrm{cap}(E) = 0$.

Théorème 3. *Pour tout compact $E \subseteq \mathbb{C}$, $\mathrm{cap}(E) = d(E)$.*

Idée de démonstration. On définit $v_n(z) = g(z) - \frac{1}{n}\log\left(\frac{|t_n(z)|}{m_n}\right)$. On montre que v_n est positive sur B, puis on prend la limite $z \to \infty$ pour obtenir $m_n^{1/n} \geq e^{-\gamma}$.

Dans l'autre sens, on montre d'abord

$$g(z) - \gamma = \frac{1}{2\pi}\int_{\partial B} \log|w - z| \frac{\partial g}{\partial n}(w)\mathrm{d}s$$

et on approxime l'intégrale par $\dfrac{1}{n}\displaystyle\sum_{k=1}^{n} \log|\zeta_k - z|$ pour des $\zeta_k \in \partial B$ bien choisis.

On montre ensuite que pour tout $\lambda > 0$, la différence entre l'intégrale et la somme converge vers 0 quand $n \to \infty$, uniformément en $z \in g^{-1}(]\lambda, \infty[)$. On en déduit que $m_n^{1/n} \leq e^{2\lambda - \gamma}$ pour n assez grand, puis on prend les limites $n \to \infty$ et $\lambda \to 0$.

La preuve est présentée de manière plus détaillée dans [Gol69]. □

2.2 Désymétrisation

La notion de capacité, utilisée en théorie du potentiel, va ici nous permettre d'étudier le comportement du diamètre transfini suite à une opération de désymétrisation, telle qu'introduite par Dubinin dans [Dub14].

Dans toute cette partie, on fixe $n \geq 2$, et $L_1^*, \ldots, L_n^*$ des demi-droites dans $\mathbb{C}$ qui partent de l'origine à des angles égaux. On appelle Φ le groupe des symétries

de $\mathbb{C}$ par rapport à ces demi-droites et à leurs bissectrices, autrement dit Φ est le groupe diédral D_n. Toutes les notions de symétries définies ci-dessous sont à comprendre comme des symétries par rapport à Φ.

Définition 8.

- On dit qu'un ensemble $A \subseteq \mathbb{C}$ est *symétrique* si $\forall \phi \in \Phi,\ \phi(A) = A$.
- Une *décomposition* est un ensemble de secteurs angulaires fermés $P_1, \dots, P_l$, dont le sommet est à l'origine, tels que $\bigcup_{j=1}^{l} P_j = \mathbb{C}$ et satisfaisant $\forall j \neq k,\ \mathring{P}_j \cap \mathring{P}_k = \emptyset$.
- Une décomposition $P_1, \dots, P_l$ est dite *symétrique* si

$$\forall \phi \in \Phi,\ \{P_1, \dots, P_l\} = \{\phi(P_1), \dots, \phi(P_l)\}.$$

Définition 9. Soit $P_1, \dots, P_l$ une décomposition symétrique. On appelle *désymétrisation* des P_j un ensemble de rotations $(\lambda_j)_{1 \leq j \leq l}$, $\lambda_j = e^{i\theta_j}$, satisfaisant :

- $S_1, \dots, S_l$ est une décomposition de $\mathbb{C}$, où $S_j = \lambda_j(P_j)$
- Si $S_j \cap S_k$ est non vide, alors

$$\exists\, \phi \in \Phi \quad \phi(\lambda_j^{-1}(S_j \cap S_k)) = \lambda_k^{-1}(S_j \cap S_k).$$

Un exemple de décomposition symétrique et de désymétrisation est illustré dans la figure 1, dans le cas $n = 4$.

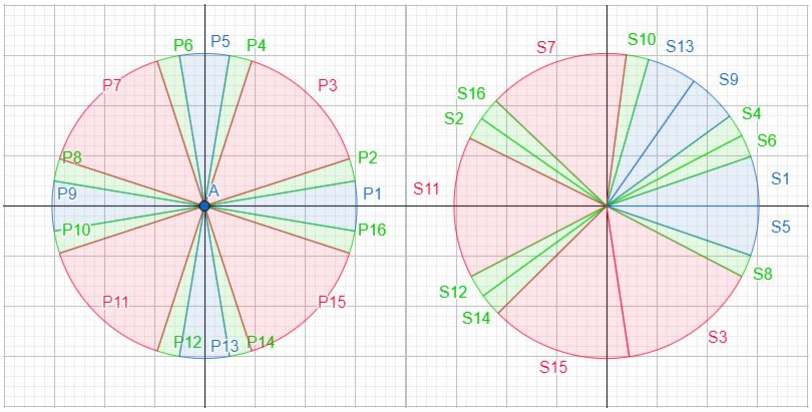


FIGURE 1 – A gauche, une décomposition symétrique. A droite, une désymétrisation possible de cette décomposition.

Définition 10. Soit $A \subseteq \mathbb{C}$ un ensemble symétrique et soit $(\lambda_j)_{1 \leq j \leq l}$ une désymétrisation d'une décomposition symétrique $(P_j)_{1 \leq j \leq l}$. On définit l'ensemble $\operatorname{Dis} A$, (pour *dissymmetrization*) par

$$\operatorname{Dis} A = \bigcup_{j=1}^{l} \lambda_j(A \cap P_j)$$

La désymétrisation d'un ensemble symétrique est illustré dans la figure 2, qui reprend la décomposition et la désymétrisation de la figure 1.

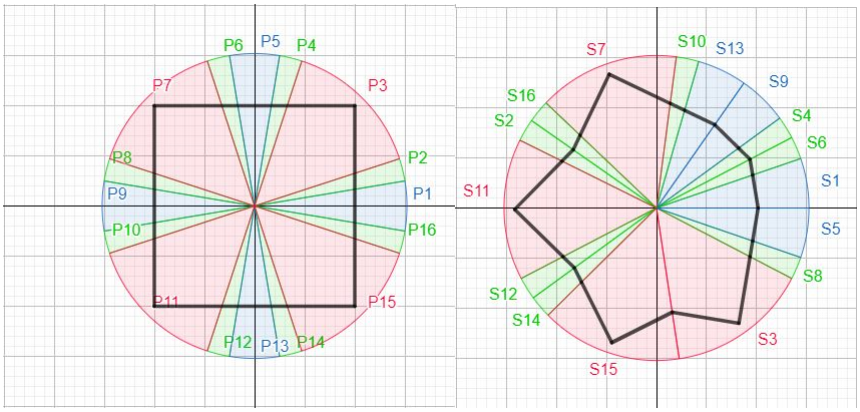


FIGURE 2 – A gauche, une décomposition et un compact symétriques. A droite, une désymétrisation de la décomposition, et la désymétrisation du compact correspondante.

Remarque. On note $\operatorname{Dis} A$, mais il faut garder en tête que la désymétrisation dépend du choix des P_j et des λ_j ! On garde cependant cette notation ambiguë car on ne considérera qu'une seule désymétrisation à la fois.

Remarque. La seconde condition dans la définition 9 n'est pas automatique, elle permet d'assurer que la frontière de $\operatorname{Dis} A$ se "recolle" de manière continue, comme on peut le voir sur la figure 2.

Pour un exemple de non-désymétrisation, on peut considérer la décomposition de la figure 1, et les rotations qui ne font qu'échanger les secteurs P_3 et P_4 entre eux. Alors la figure obtenue ne respecte pas la seconde condition de la définition.

L'existence de décompositions non triviales est assurée par la proposition suivante, tirée de [Dub14] :

Proposition 5. *Soient $L_1, \dots, L_n$ des demi-droites distinctes partant de l'origine. On rappelle qu'on a défini $L_1^*, \dots, L_n^*$ comme étant des demi-droites partant de l'origine à des angles égaux.*

Il existe une décomposition symétrique (P_j) et une désymétrisation (λ_j) tels que, pour tout $k \leq n$, $\operatorname{Dis} L_k^* = L_k$.

2.3 Le théorème de Dubinin

Théorème 4 (Dubinin)**.** *Soit $E \subseteq \mathbb{C}$ un compact symétrique, soit (P_j) une décomposition symétrique, et soit (λ_j) une désymétrisation. Alors*

$$\operatorname{cap}(E) \geq \operatorname{cap}(\operatorname{Dis} E).$$

Idée de démonstration. La démonstration peut être trouvée dans la Section 4.4 de [Dub14], elle repose sur la notion de capacité d'un condensateur. Un *condensateur* estne paire (E_0, E_1) de deux fermés non vides disjoints. La *capacité d'un condensateur* est

$$\operatorname{cap}(E_0, E_1) = \inf\{I(v, D) \mid v \in \operatorname{Lip},\ v = i \text{ on } E_i\}$$
$$\text{où} \qquad I(v, D) = \int_D \left(\frac{\partial v}{\partial x}\right)^2 + \left(\frac{\partial v}{\partial y}\right)^2 \mathrm{d}x\mathrm{d}y$$

est l'intégrale de Dirichlet et où $D = \mathbb{C} \setminus (E_0 \cup E_1)$. On montre que si E_0, E_1, D sont symétriques, on peut se restreindre à demander v symétrique dans la définition de capacité d'un condensateur.

Pour la preuve, on définit $C(\infty, r) = \{z \in \mathbb{C} \mid |z| \geq 1/r\}$, et $C_E(r) = (E, C(\infty, r))$. Un lemme, dont la démonstration peut se trouver dans [Hay94], affirme

$$\frac{2\pi}{\operatorname{cap} C_E(r)} = -\log r - \log \operatorname{cap} E + o(1) \quad \text{quand } r \to 0,$$

ce qui permet de relier la capacité du condensateur à la capacité du compact qui nous intéresse.

Le théorème suit en découpant le compact E suivant la décomposition et en appliquant la désymétrisation. □

3 Diamètre transfini dans $\mathbb{C}_p$ et théorème de Bertrandias

Le théorème de Bertrandias va nous permettre de transformer la notion géométrique de diamètre transfini en la notion algébrique de rationalité d'une série entière. Pour cela, nous avons tout d'abord besoin de parler de nombres p-adiques.

3.1 Prolongement analytique dans $\mathbb{C}_p$

On rappelle que $\mathbb{Q}_p$ est l'ensemble des nombres p-adiques, complétion de $\mathbb{Q}$ par rapport à la valeur absolue $|\,.\,|_p$, et que $\mathbb{C}_p$ est la complétion de la clôture algébrique de $\mathbb{Q}_p$. La valeur absolue de $\mathbb{Q}_p$ s'étend de manière unique sur $\mathbb{C}_p$, et équipé de cette valeur absolue, $\mathbb{C}_p$ est complet algébriquement clos. On peut donc le voir comme l'équivalent de $\mathbb{C}$ dans le cadre p-adique.

Pour plus de détails sur les nombres p-adiques, on pourra se référer par exemple à [Gou03] ou à [Rob00].

Dans $\mathbb{C}$, on a la notion de prolongement analytique : soit f une fonction holomorphe, développable en série entière en 0 sur un disque de rayon R. En prenant un point $z_0 \neq 0$ dans ce disque et en développant f en série entière

autour de ce point, il peut arriver que le nouveau disque de convergence n'est pas inclus dans l'ancien. On a ainsi prolongé f analytiquement à un domaine plus grand.

Dans $\mathbb{C}_p$, cette construction n'est pas possible. En effet, la valeur absolue sur $\mathbb{C}_p$ est non-archimédienne, une conséquence de cela est que le domaine de convergence reste le même, peu importe le point z_0 choisi.

Pour pallier à cela, on a la définition suivante, introduite dans [Kra54], qui s'inspire du théorème de Runge sur $\mathbb{C}$:

Définition 11. Soit $D \subseteq \mathbb{C}_p$ un ouvert. On dit qu'une fonction $f : D \to \mathbb{C}_p$ est un *élément analytique* si f est limite de fractions rationnelles, sans pôles dans D, et qui convergent uniformément vers f.

Si $A \subseteq D$ est ouvert, $g : A \to \mathbb{C}_p$ peut être *prolongée analytiquement* à D s'il existe un élément analytique sur D qui coïncide avec g sur A.

On aimerait voir que ces éléments analytiques sont une généralisation des séries entières, c'est le contenu de la :

Proposition 6. *Soit $f : D \to \mathbb{C}_p$ un élément analytique, où D est un disque ouvert $B(a, R)$ (resp. une couronne $C(a, r, R) := \{x \in \mathbb{C}_p \mid r < |x| < R\}$). Alors f est égal à la somme d'une série entière (resp. série de Laurent) centrée en a.*

3.2 Diamètre transfini dans un corps valué

Dans les sections précédentes, on s'est intéressé uniquement au diamètre transfini dans $\mathbb{C}$, mais on peut en fait en donner une définition dans un corps valué arbitraire.

Définition 12. Soit $(K, |\,.\,|)$ un corps valué, soit $E \subseteq K$ un ensemble borné. On définit le diamètre transfini de E dans K comme étant la limite de la suite

$$d_n = \left(\sup_{z_1,\dots,z_n \in E} \prod_{1 \leq i < j \leq n} |z_i - z_j| \right)^{\frac{2}{n(n-1)}}$$

On le note $d_K(E)$.

La seule différence avec la définition précédente est que le max est devenu un sup, puisqu'on suppose ici seulement que E est borné. Le fait que la suite (d_n) converge se montre exactement comme dans le cas précédent. En fait la plupart des propositions précédentes sont encore valables :

- La proposition 1 est valable.
- Si on définit m_n comme précédemment (en remplaçant les max/min par des sup/inf), alors $m_n^{1/n}$ converge vers la constante de Tchebychev $\tau_K(E)$.
- $d_K(E) = \tau_K(E)$.
- La proposition 4 est valable, à condition de supposer K algébriquement clos.

3.3 Le théorème de Bertrandias

Théorème 5 (Bertrandias)**.** *Soit K un corps de nombres, soit V l'ensemble de ses places non-archimédiennes, et soit S un sous-ensemble fini de V. On considère*

$$f = \sum_{i=1}^{\infty} a_i/X^i \in K[[1/X]]$$

une série de Laurent à coefficients dans K. On suppose :

1. $\forall n \geq 1,\ \forall v \in V \setminus S,\quad |a_n|_v \leq 1$
2. *Pour $v \in S$, f, vue comme fonction d'une variable dans $\mathbb{C}_p$, peut être prolongée analytiquement au complémentaire d'un fermé borné $A_v \subseteq \mathbb{C}_v$ (dans le sens de la définition 11).*
3. *Pour tout $\sigma : K \hookrightarrow \mathbb{C}$, la série de Laurent $\sum \sigma(a_i)/X^i$ peut être prolongée analytiquement au complémentaire d'un compact $A_\sigma \subseteq \mathbb{C}$ (dans le sens usuel).*
4. $\displaystyle\prod_{\sigma : K \hookrightarrow \mathbb{C}} d_{\mathbb{C}}(A_\sigma) \prod_{v \in S} d_{\mathbb{C}_v}(A_v) < 1.$

Alors f est une fraction rationnelle.

La démonstration s'appuie sur le résultat suivant, attribué à Kronecker :

Proposition 7. *Soit $f = \displaystyle\sum_{i=1}^{+\infty} a_i X^i \in K[[X]]$ une série entière avec des coefficients à valeurs dans un corps K. On note $D_n(f)$ le déterminant de la matrice $(a_{i+j-1})_{1 \leq i,j \leq n}$. Alors f est une fraction rationnelle si et seulement si il existe $N \in \mathbb{N}$ tel que $\forall n \geq N, D_n(f) = 0$.*

Idée de démonstration du théorème 5. On aimerait montrer

$$\limsup |D_n(f)|_\sigma^{1/n^2} \leq d_{\mathbb{C}}(A_\sigma) \qquad \text{et} \qquad \limsup |D_n(f)|_v^{1/n^2} \leq d_{\mathbb{C}_v}(A_v)$$

pour $\sigma : K \hookrightarrow \mathbb{C}$ et $v \in S$ respectivement. Si ces inégalités sont vraies, l'hypothèse 4 et la formule du produit amènent à $D_n(f) = 0$ pour n assez grand, et la proposition 7 permet de conclure.

Pour prouver ces inégalités, l'idée est de prendre des ε-polynômes de Tchebychev pour approximer le diamètre transfini, puis d'exprimer $D_n(f)$ en fonction de ces polynômes par des combinaisons linéaires des lignes/colonnes.

La preuve complète peut être trouvée dans [Ber63] ou dans [Ami75]. □

Le théorème de Bertrandias ne va nous intéresser que dans un cas particulier, à savoir $K = \mathbb{Q}$ et $S = \emptyset$. On obtient alors le corollaire suivant :

Corollaire 1. *Soit $f = \displaystyle\sum_{i=0}^{\infty} a_i/X^i \in \mathbb{Z}[[1/X]]$ une série de Laurent à coefficients entiers. Si f peut être prolongée analytiquement au complémentaire d'un compact $K \subseteq \mathbb{C}$ dont le diamètre transfini satisfait $d(K) < 1$, alors f est rationnelle.*

Le théorème et le corollaire nous disent qu'une série entière en $1/X$ dont les coefficients sont (presque) entiers ne peut pas converger sur un ensemble "trop gros" sans être un polynôme en $1/X$. La notion de "trop gros" est cependant obtenue ici de manière assez subtile puisqu'elle fait intervenir le diamètre transfini.

4 Preuve de la conjecture de Schinzel-Zassenhaus

On donne dans cette section la preuve de la conjecture de Schinzel-Zassenhaus, selon Dimitrov. Le contenu de cette section est intégralement tiré de [Dim19].

On remarque tout d'abord que dans l'énoncé du théorème, le seul problème avec $n = 1$ est le polynôme $P(X) = X$. On va donc prouver le théorème pour $n \geq 1$ en rajoutant l'hypothèse $P(X) \neq X$.

4.1 Notations et lemmes

Définition 13. On définit les polynômes auxiliaires suivants :

— pour $m \geq 1, P_m(X) = \prod_{i=1}^{n}(X - \alpha_i^m) \in \mathbb{Z}[X]$

— $P^*(X) = X^n P(1/X)$ est le polynôme réciproque de P.

Définition 14. Si on se donne k points $a_1, \dots a_k \in \mathbb{C}$, on définit le *hérisson* associé à ces points comme étant l'union des segments reliant l'origine à ces points :

$$\mathcal{K}(a_1, \dots, a_k) = \bigcup_{i=1}^{k}[0, a_i]$$

On commence par quelques lemmes :

Lemme 1. *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire. On a la relation de congruence $P_4 \equiv P_2 \mod 4\,\mathbb{Z}[X]$.*

Lemme 2. *La série de Taylor de $\sqrt{1+4Y}$ a des coefficients entiers.*

Lemme 3. *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible. Si $\sqrt{P_2 P_4}$ est une fraction rationnelle, alors ou bien P est cyclotomique, ou bien P_2 est un carré dans $\mathbb{Z}[X]$.*

Démonstrations. La preuve des lemmes 1 et 3 est présentée dans [Dim19]. Le lemme 2 se prouve par un calcul explicite, ou bien en utilisant l'astuce présentée dans [Lub12]. □

4.2 Démonstration du théorème 1

On fait la preuve par récurrence sur le degré n.

Si $n = 1$, alors $P = X - a$, et a n'est ni 0 ($P(X) \neq X$), ni ± 1 (P n'est pas cyclotomique), donc $|a| \geq 2 \geq 2^{1/4}$.

Soit $n \geq 2$ et supposons le théorème vrai pour tout degré $k < n$. Soit P satisfaisant les hypothèses du théorème. On définit

$$f(X) = \sqrt{P_2^*(1/X)P_4^*(1/X)}.$$

On veut appliquer le corollaire du théorème de Bertrandias à f.

Grâce au lemme 1, $P_2 \equiv P_4 \mod 4$, donc $P_2^* \equiv P_4^* \mod 4$, et donc il existe un polynôme R tel que

$$P_2^*(X)P_4^*(X) = P_2^*(X)^2 + 4R(X)$$

Comme P est supposé unitaire, $P_2^*(0) = P^*(0)^2 = 1$ et $P_4^*(0) = 1$, donc $R(0) = 0$. On a donc

$$\sqrt{P_2^*(X)P_4^*(X)} = P_2^* \sqrt{1 + 4\frac{R(X)}{P_2^*(X)^2}} \in \mathbb{Z}[[X]]$$

en appliquant le lemme 2 avec $Y = \dfrac{R(X)}{P_2^*(X)^2}$. Ainsi $f(X) \in \mathbb{Z}[[1/X]]$.

De plus les points de ramification de f se trouvent lorsque l'intérieur de la racine est nul. Cela correspond aux points α_i^2 et α_i^4. On en déduit que f est prolongeable analytiquement au complémentaire de tout compact connexe contenant ces points. On choisit ici le hérisson à $2n$ branches $\mathcal{K}(\alpha_i^2, \alpha_i^4)$.

Notons $M = \max |\alpha_i|^4$, alors

$$\begin{aligned} d(\mathcal{K}(\alpha_i^2, \alpha_i^4)) &\leq d\left(\mathcal{K}\left(\frac{M}{|\alpha_i^2|}\alpha_i^2, \frac{M}{|\alpha_i^4|}\alpha_i^4\right)\right) \\ &= M\, d\left(\mathcal{K}\left(\frac{\alpha_i^2}{|\alpha_i^2|}, \frac{\alpha_i^4}{|\alpha_i^4|}\right)\right). \end{aligned}$$

La première inégalité consiste à rallonger la longueur des branches pour qu'elles aient toutes longueur M, puis utiliser la proposition 1.3 (inclusion). L'égalité vient de la proposition 1.5.

Le dernier hérisson qui apparaît est, d'après la proposition 5, une désymétrisation d'une étoile régulière à $2n$ branches, dont le diamètre transfini est $\dfrac{1}{4^{1/2n}}$, calculé dans l'exemple juste après la proposition 4.

D'après le théorème de Dubinin,

$$d(\mathcal{K}(\alpha_i^2, \alpha_i^4)) \leq \frac{M}{4^{1/2n}} = \frac{\max |\alpha_i|^4}{2^{1/n}}$$

Supposons par contradiction que $\max |\alpha_i| < 2^{1/4n}$. Alors $d(\mathcal{K}(\alpha_i^2, \alpha_i^4)) < 1$. On peut donc utiliser le corollaire 1 du théorème de Bertrandias : $f(X)$ est une fraction rationnelle.

Donc $\sqrt{P_2(X)P_4(X)} = X^n f(X)$ est également rationnel. Comme P est supposé non-cyclotomique, le lemme 3 implique que $P_2 = Q^2$ pour un certain polynôme Q. Or $P_2 = \prod(X - \alpha_i^2)$, et les α_i sont distincts, P étant irréductible. Quitte à les réordonner, les racines de P sont donc $\alpha_1, -\alpha_1, \ldots, \alpha_{n/2}, -\alpha_{n/2}$. Donc $Q = \prod_{i=1}^{n/2}(X - \alpha_i^2)$.

Q satisfait toutes les hypothèses du théorème et est de degré $n/2$. D'après l'hypothèse de récurrence, on a donc

$$\max |\alpha_i|^2 \geq 2^{\frac{1}{2n}}$$

ce qui contredit $\max |\alpha_i| < 2^{1/4n}$, et finit de prouver le théorème. □

5 Discussion de résultats additionnels

Dans cette section, on discute d'idées pouvant conduire à des généralisations du théorème prouvé par Dimitrov. Les deux idées discutées sont les suivantes : une généralisation à un corps de nombres, et l'amélioration de la constante $\log 2/4$.

5.1 Généralisation à un corps de nombres

Au vu de la preuve proposée par Dimitrov, une question naturelle à se poser est la suivante : qu'y a-t-il de spécial avec P_2 et P_4 ? En fait, en suivant la même preuve, on montre que pour tout nombre premier p, on a sous les mêmes hypothèses que le théorème 1 :

$$\max |\alpha_i| \geq 2^{1/p^2 n}.$$

Cependant cette borne est la meilleure pour $p = 2$, ce qui correspond au théorème.

Les polynômes P_p et P_{p^2} pourraient néanmoins avoir un rôle à jouer si on essaye de généraliser le théorème 1 à l'anneau des entiers d'un corps de nombres. En effet, dans un corps de nombres K, un nombre premier $p \in \mathbb{Z}$ peut avoir différents comportements (être scindé, ramifié, inerte, ...), qui peuvent se comporter plus ou moins bien avec la preuve actuelle. De plus, l'idée d'une généralisation à un corps de nombres semble prometteuse vu que le théorème de Bertrandias (théorème 5) a un énoncé plus général que le corollaire qu'on a utilisé.

Dimitrov présente donc dans son article un *Théorème 2*, généralisation de la conjecture de Schinzel-Zassenhaus. Cependant, en étudiant la preuve de ce second théorème, j'ai découvert plusieurs problèmes, que je n'ai pu corriger que de manière incomplète. Après en avoir discuté avec mon maître de stage, j'ai écrit une note à l'attention de l'auteur explicitant les problèmes, les contre-exemples et les solutions partielles que j'ai pu trouver. J'ai inclus cette note en

annexe A. Au moment d'écrire ce rapport, je n'ai toujours pas de nouvelles de l'auteur si ce n'est une promesse (datant de deux mois) de me recontacter dans quelques jours.

Une généralisation aux corps de nombres semble donc possible, mais reste encore à préciser.

5.2 Amélioration de la constante

Une autre question que l'on peut se poser est : « quelle est la meilleure constante possible telle que la conjecture de Schinzel-Zassenhaus soit vraie ? »

Plus formellement, on cherche à déterminer

$$\begin{aligned} c_0 &:= \sup\left\{ c > 0 \mid \forall P \in \mathcal{Q},\ \max_{\alpha\,:\,P(\alpha)=0} |\alpha| \geq 1 + \frac{c}{\deg P} \right\} \\ &= \inf_{P\in\mathcal{Q}} \left(\left(\max_{\alpha\,:\,P(\alpha)=0} |\alpha| - 1 \right) . \deg P \right) \end{aligned}$$

où $\mathcal{Q} = \{P \in \mathbb{Z}[X] \mid P$ unitaire, irréductible, non-cyclotomique, $\deg P \geq 2\}$ est l'ensemble des polynômes satisfaisant les hypothèses du théorème.

La meilleure borne inférieure dont on dispose actuellement est celle prouvée par Dimitrov :

$$c_0 \geq \frac{\log 2}{4} \approx 0.17$$

On peut néanmoins s'intéresser à une borne supérieure :

— Le choix le plus simple est de considérer la famille $P_n = X^n - 2 \in \mathcal{Q}$. Alors $\max|\alpha| = \sqrt[n]{2} = 1 + \frac{\log 2}{n} + O(\frac{1}{n^2})$, et donc $c_0 \leq \log 2$.

— Un autre choix qui semble plus raffiné est de considérer les polynômes $P_n = X^n - X - 1$. On montre que P_n est irréductible, et qu'il possède une seule racine réelle positive θ_n, qui est la racine dont le module est maximal. Cependant, au final la borne n'est pas améliorée, car on a $\theta_n = 1 + \frac{\log 2}{n} + O(\frac{1}{n^2})$, et on obtient comme précédemment $c_0 \geq \log 2$.

— Ce dernier exemple, tiré de [Smy71] consiste à considérer $P_n = -P^*(X^n)$, où $P = X^3 - X - 1$. On montre que P_n est irréductible, $\deg P_n = 3n$. De plus, si on note $\theta \approx 1.32$ la racine réelle positive de P, alors on a

$$\max_{\alpha\,:\,P_n(\alpha)=0} |\alpha| = \theta^{1/2n} = 1 + \frac{3/2 \log\theta}{3n} + O(\frac{1}{n^2}),$$

ce qui donne au final la borne $c_0 \leq \dfrac{3}{2}\log\theta \approx 0.43$.

Il est supposé que cette dernière borne est en fait la "vraie" valeur de c_0. Cette conjecture est en partie appuyée par les calculs explicites en petit degré de [Boy85].

Conclusion

La preuve de Dimitrov est loin d'être une preuve classique, elle se distingue notamment par son usage extensif de la notion de diamètre transfini. Cette approche semble très prometteuse, et pourrait permettre d'aboutir à de nouveaux résultats en théorie des nombres. On pense notamment à la conjecture de Lehmer, qui est fondamentalement proche de la conjecture de Schinzel-Zassenhaus.

Le diamètre transfini semble jouer un certain rôle dans des domaines assez distincts des mathématiques. Une suite possible du travail de ce stage pourrait être d'étudier un phénomène qui est apparu lors de nos discussions avec Fabien Pazuki : il semble y avoir un lien entre le diamètre transfini des polygones réguliers et la période de certaines courbes elliptiques à multiplication complexe.

A Remarks about Theorem 2 of V. Dimitrov's preprint arxiv1912.12545

While studying V. Dimitrov's preprint https ://arxiv.org/pdf/1912.12545.pdf, I came across a few points that are not clear (maybe not correct) concerning Theorem 2. After discussing these points in depth, I made this note where I expose them in detail.

Typo. In the statement of Lemma 2.7, it should be "Suppose that $P_p(X)$ is NOT a perfect p-th power" instead of "Suppose that $P_p(X)$ is a perfect p-th power", since in the proof P_p is assumed to be irreducible.

Problem 1. In lemma 2.5, the following congruence relation is proven :

$$P_{p^2} \equiv P_{p^e}^{\kappa} \mod p^2.O_p[X] \tag{1}$$

with $e = 1$ or 2 depending whether p is unramified or ramified in F, respectively. However, in the proof of Proposition 2.6, the following statement is made :

$$P_{p^e}(X)^{p-1} P_{p^2}(X)^{\kappa} \equiv P_{p^e}(X)^p \mod p^2 \tag{2}$$

Between equation 1 and equation 2, the indices p^2 and p^e have been switched, and the latter equation becomes false :

Counterexample. Take $\zeta = e^{2i\pi/5}$, $F = \mathbb{Q}(\zeta)$, $p = 3$ and $P = X - \zeta \in O_F[X]$.

In this setup, p is unramified in F so we have $e = 1$ and $\kappa : \zeta \mapsto \zeta^p = \zeta^3$. Then :

$$\begin{aligned} P_p(X)^{p-1} P_{p^2}^{\kappa} &= (X - \zeta^3)^2 (X - \kappa(\zeta^9)) = (X - \zeta^3)^2 (X - \zeta^2) \\ P_p(X)^p &= (X - \zeta^3)^3 \end{aligned}$$

which are not congruent modulo $9 = p^2$.

Solution. Given Lemma 2.5, the right congruence relation to use would be

$$P_{p^2}(X)^{p-1} P_{p^e}(X)^{\kappa} \equiv (P_{p^e}(X)^{\kappa})^p \mod p^2$$

Following the same proof, this leads to the v-adic disk $|X|_v < \left(\dfrac{|\kappa(c_0)|_v}{\max |\kappa(c_i)|_v} \right)^{p^{e+1}}$ instead of $|X|_v < \left(\dfrac{|c_0|_v}{\max |c_i|_v} \right)^{p^{e+1}}$, which is unfortunately less convenient.

Problem 2. In the middle of the proof of Proposition 2.6, a claim is made that

$$\frac{b_0 |Q|_v}{Q(b_0 |Q|_v X)} \in O_{\mathbb{C}_v}[[X]]$$

where $Q = \sum_{i=0}^{n} b_i X^i$, $b_0 \neq 0$, $|Q|_v = \max |b_i|_v$. This is not the case :

Counterexample. Take $F = \mathbb{Q}$, $v = 5$, $Q(X) = 5 - 5X$. Then $|Q|_v = 1/5$ and

$$\frac{b_0|Q|_v}{Q(b_0|Q|_v X)} = \frac{5\ .\ 1/5}{5 - 5(5\ .\ 1/5\ .\ X)} = \frac{1}{5}(1 + X + X^2 + ...) \notin O_{\mathbb{C}_v}[[X]]$$

Solution. A first solution would be to ask for $|Q|_v = 1$.

Another solution would be to do the proof using instead the integrality of $\dfrac{b_0}{Q(b_0 X)} \in O_{\mathbb{C}_v}[[X]]$, at the cost of a worse bound in Proposition 2.6.

Problem 3. In the proof of proposition 2.6, it is claimed that

$$P_{p^e}(X)^{p-1} P^{\kappa}_{p^2}(X) = P_{p^e}(X)^p + p^2 H(X) \quad \text{with } H(0) = 0.$$

The corresponding claim after taking into account the modifications due to Problem 1 above is :

$$P_{p^2}(X)^{p-1} P^{\kappa}_{p^e}(X) = P^{\kappa}_{p^e}(X)^p + p^2 H(X) \quad \text{with } H(0) = 0. \tag{3}$$

However, in both cases, there is no reason for H to satisfy $H(0) = 0$.

Counterexample. Take $F = \mathbb{Q}$, $P = X^2 - 2$, $p = 2$. Then $e = 1$, $\kappa = \mathrm{Id}$, $P_2 = (X-2)^2$, $P_4 = (X-4)^2$, and :

$$(P^{p-1}_{p^2} P^{\kappa}_{p^e} - (P^{\kappa}_{p^e})^p)(0) = (P_4 P_2 - P_2^2)(0) = 16\ .\ 4 - 16 = 48 \neq 0.$$

Note that since $\kappa = \mathrm{Id}$, this is also a counterexample for the original claim.

Solution. By direct computation, we can see that equation 3 is true if $P(0) = 1$. The polynomial P we are using here is the reciprocal polynomial of the polynomial involved in Theorem 2 (rescaled to have integer coefficients). Asking for $P(0) = 1$ in equation 3 amounts to asking for the polynomial in Theorem 2 to be monic and with coefficients in O_p.

Note that this solution solves efficiently the three problems above, indeed with this hypothesis we have $|Q|_v = 1$ which solves Problem 2, and we don't need an explicit radius for the v-adic disc since $c_{P/K} = 1$, which solves Problem 1.

Problem 4. The proof of Theorem 2 involves an induction, however no base case is proven for this induction, and I can't see an easy way of proving one.

Références

[Ami75] Y. Amice. *Les nombres p-adiques*. T. 14. Collection Sup Le Mathématicien. Paris : Presses universitaires de France, 1975.

[Ber63] F. Bertrandias. « Diamètre transfini dans un corps valué. Application au prolongement analytique ». In : *Séminaire Delange-Pisot-Poitou* 5 (1963).

[Boy85] D. W. Boyd. « The Maximal Modulus of an Algebraic Integer ». In : *Mathematics of Computation* 45.171 (1985), p. 243-249.

[Dim19] V. Dimitrov. *A proof of the Schinzel-Zassenhaus conjecture on polynomials*. 2019. arXiv : `1912.12545 [math.NT]`.

[Dob79] E. Dobrowolski. « On a question of Lehmer and the number of irreducible factors of a polynomial ». In : *Acta Arithmetica* 34.4 (1979), p. 391-401.

[Dub14] V. N. Dubinin. *Condenser Capacities and Symmetrization in Geometric Function Theory*. Springer Basel, 2014. Chap. 1, 2, 4.4.

[Gol69] G. M. Goluzin. *Geometric theory of functions of a complex variable*. T. 26. American Mathematical Society, 1969, p. 293-313.

[Gou03] F. Q. Gouvêa. *p-adic Numbers : An Introduction*. Universitext. Springer Berlin Heidelberg, 2003.

[Hay65] W. K. Hayman. « Lectures on Transfinite Diameter and its Applications. » In : *MatScience Report* 45 (1965).

[Hay94] W. K. Hayman. *Multivalent Functions*. 2e éd. Cambridge Tracts in Mathematics. Cambridge University Press, 1994. Chap. 4.

[Kra54] M. Krasner. « Prolongement analytique dans les corps valués complets ». In : *Comptes rendus de l'Académie des Sciences* 239 (1954), p. 468-470, 745-747.

[Lub12] J. Lubin. *Fractional Binomial Coefficients*. Mathematics Stack Exchange. 2012. url : `https://math.stackexchange.com/q/168833`.

[Rob00] A. M. Robert. *A Course in p-adic Analysis*. Graduate Texts in Mathematics. Springer New York, 2000.

[Smy71] C. Smyth. « On the Product of the Conjugates outside the unit circle of an Algebraic Integer ». In : *Bulletin of the London Mathematical Society* 3 (1971), p. 169-175.

[SZ65] A. Schinzel et H. Zassenhaus. « A refinement of two theorems of Kronecker. » In : *Michigan Math. J.* 12.1 (1965), p. 81-85.