Inégalités de Hurwitz pour les corps de nombres

A. L. Smirnov

1992

On étudie un analogue en théorie des nombres de la formule de Hurwitz pour le revêtement d'une courbe algébrique. On introduit un objet qui remplace en partie la droite projective sur le corps des constantes, et on formule une inégalité de Hurwitz hypothétique. On construit plusieurs séries d'exemples montrant la précision asymptotique de cette inégalité. On montre que l'inégalité de Hurwitz entraîne la conjecture ABC, l'inégalité de Szpiro sous la forme de Parshin, etc. En conclusion, on discute des voies possibles de développement de la théorie.

Introduction

Dans le présent travail, il est question d'un analogue en théorie des nombres de la formule classique de Hurwitz. Pour une courbe algébrique lisse X sur un corps k, une fonction rationnelle $f \in k(X)$ peut être considérée comme un morphisme $f : X \to \mathbb{P}^1$. Si $f \neq \text{const}$ et si le corps $k(X)$ est séparable sur le corps $k(\mathbb{P}^1)$, alors la formule de Hurwitz suivante est valable :

$$\chi(X) = 2 \deg f - \sum_{P \in X} v_P(D_f) \deg P.$$

Le premier paragraphe est consacré à la discussion de cette formule dans le contexte qui convient pour le reste du travail.

Par analogie classique, le corps de nombres K doit être considéré comme le corps des fonctions rationnelles sur l'espace de tous les points du corps K, y compris les points archimédiens. Cependant, dans le cas numérique, contrairement au cas géométrique, il n'y a pas de corps de constantes, ni a fortiori de droite projective sur celui-ci. Au § 2, on introduit un certain objet qui remplace, dans une certaine mesure, la droite projective. Ensuite, on introduit les analogues numériques des autres quantités intervenant dans la formule de Hurwitz.

La manière dont il faut définir la différente complète n'est pas tout à fait claire, mais il est facile de définir sa partie modérée. Après cela, au lieu de la formule de Hurwitz, on peut formuler une inégalité de Hurwitz hypothétique. Cela est fait au § 3.

Au § 4, on construit cinq séries différentes d'exemples montrant la précision asymptotique de l'inégalité de Hurwitz. Deux d'entre elles sont liées à des courbes rationnelles (tore et conique), et trois à des courbes elliptiques (cubique de Fermat, quartique de Jacobi, paire de quadriques sous la forme de Mumford). En outre, on donne ici un résultat de Stewart et Tijdeman, qui donne la meilleure estimation connue de l'auteur pour le terme complémentaire.

Au § 5, on donne quelques conséquences de l'inégalité de Hurwitz numérique :

(1) la conjecture ABC de Masser et Oesterlé ;

(2) l'inégalité de Szpiro sous la forme de Parshin ;

(3) une estimation de l'ordre d'approximation des logarithmes par des nombres rationnels ;

(4) une estimation de la croissance des nombres premiers singuliers p, c'est-à-dire les nombres p pour lesquels $f^p \equiv f \pmod{p^2}$ (f est un nombre rationnel fixé).

Notons que dans le cas du corps $\mathbb{Q}$, l'inégalité de Hurwitz est un renforcement de la conjecture ABC connue de Masser et Oesterlé. Bien qu'actuellement aucun moyen de démontrer cette conjecture ne soit en vue, il y a quelques raisons pour son raffinement ultérieur. Le pas le plus radical dans cette direction est l'hypothèse de l'existence d'une formule de Hurwitz exacte.

$$\boxed{\text{Conjecture ABC}} \Leftarrow \boxed{\text{Inégalité de Hurwitz}} \Leftarrow \boxed{\text{? Formule de Hurwitz}}$$

En conclusion, on discute de quelques problèmes de la théorie et des voies possibles de leur résolution, on pose quelques questions.

L'auteur exprime sa reconnaissance à A. N. Parshin pour son soutien et ses conseils utiles, ainsi que sa joie de remercier ses amis I. A. Panin, I. M. Khamitov, S. A. Evdokimov et M. M. Kapranov pour leurs nombreuses discussions.

§ 1. Cas fonctionnel

Dans ce paragraphe, on formule quelques résultats classiques de la théorie des courbes algébriques. Ces résultats sont donnés sous une forme commode pour l'examen ultérieur du cas numérique. Toutes les définitions nécessaires et les démonstrations détaillées peuvent être trouvées, par exemple, dans [1]. En outre, on donne ici la formulation d'une certaine inégalité, que l'auteur appelle inégalité de Hurwitz et qui sera utilisée par la suite comme prototype pour l'examen du cas numérique.

1.1. Formule de Hurwitz. Soit X une courbe complète lisse sur un corps k, $K = k(X)$ le corps des fonctions rationnelles sur X, $f \in K$. La fonction f peut être considérée comme un morphisme $f : X \to \mathbb{P}^1$, où $\mathbb{P}^1$ est la droite projective sur le corps k. Si $f \notin k$ et si le corps K est séparable sur le corps $k(\mathbb{P}^1)$, alors la formule de Hurwitz suivante est valable :

$$\chi(X) = 2 \deg f - \sum_{P \in X} v_P(D_f) \deg P. \tag{1.1}$$

Ici $\chi(X) = 2 - 2g(X)$ est la caractéristique d'Euler topologique de X, D_f est la différente du morphisme f, c'est-à-dire le faisceau d'idéaux sur X qui est l'annulateur du faisceau des différentielles relatives $\Omega_{X/\mathbb{P}^1}$, v_P est la valuation discrète associée au point P.

Écrivons la formule (1.1) sous une forme légèrement différente :

$$\sum_{P \in X} \frac{v_P(D_f) \deg P}{\deg f} = 2 - \frac{\chi(X)}{\deg f}. \tag{1.2}$$

On fera référence par la suite à la formule (1.2) comme à la formule de Hurwitz.

1.2. Défauts. Introduisons les notations suivantes :

$$\Delta_P = \frac{v_P(D_f)\deg P}{\deg f} - \text{défaut total au point } P,$$

$$\delta_P = \frac{(e_P - 1)\deg P}{\deg f} - \text{défaut modéré au point } P.$$

Ici e_P est l'indice de ramification de f au point P.

En vue de la discussion ultérieure du cas numérique, donnons une description élémentaire des défauts.

Soit $P \in X$, $f(P) = Q$ un point de $\mathbb{P}^1$, K_P le complété du corps K pour la topologie P-adique, u un paramètre local dans le corps K_P. Alors

$$v_P(D_f) = \begin{cases} v_P(df/du), & \text{si } Q \neq \infty, \\ v_P(d(1/f)/du), & \text{si } Q = \infty. \end{cases} \tag{1.3}$$

Soit k_P le corps résiduel au point P et, si $Q \neq \infty$, $\varepsilon = f(P) \in k_P$. Alors

$$e_P = \begin{cases} v_P(f - \varepsilon), & \text{si } Q \neq \infty, \\ v_P(1/f), & \text{si } Q = \infty. \end{cases} \tag{1.4}$$

1.3. Inégalités de Hurwitz. Par définition de s_P, l'égalité suivante est vraie :

$$v_P(D_f) = e_P - 1 + s_P.$$

On sait que $s_P \geq 0$. Par conséquent, de (1.2) découlent les inégalités

$$\begin{aligned} \sum_{P \in X} \Delta_P &\leq 2 - \frac{\chi(X)}{\deg f}, \\ \sum_{P \in X} \delta_P &\leq 2 - \frac{\chi(X)}{\deg f}. \end{aligned} \tag{1.5}$$

Dans ces inégalités, la somme du membre de gauche peut ne porter que sur une partie des points de X. Les inégalités de ce type seront appelées inégalités de Hurwitz.

Il est parfois plus commode de sommer sur les points de $\mathbb{P}^1$, c'est pourquoi pour $Q \in \mathbb{P}^1$ on pose

$$\begin{aligned} \delta_Q &= \sum_{P \to Q} \delta_P, \\ \Delta_Q &= \sum_{P \to Q} \Delta_P. \end{aligned} \tag{1.6}$$

S'il est nécessaire d'indiquer la dépendance des défauts par rapport à f, K, etc., on écrira $\delta_P(f)$, $\delta_P(f, K)$, etc.

§ 2. Position du problème dans le cas numérique

Dans ce paragraphe, nous passons au cas numérique. Au lieu du corps des fonctions sur une courbe algébrique, nous considérerons un corps de nombres K. Nous supposerons que $K \subset \overline{\mathbb{Q}}$, où $\overline{\mathbb{Q}}$ est la clôture algébrique du corps $\mathbb{Q}$. Au lieu d'une fonction sur une courbe algébrique, nous considérerons un élément f du corps K. Cependant, dans le cas numérique, un certain nombre d'objets clés sont absents, le corps des constantes, la droite projective sur celui-ci, etc. Ci-dessous, on introduit certains objets qui comblent partiellement ces lacunes.

2.1. Que prendre comme X. Conformément à l'analogie classique, comme points de X nous prendrons tous les points du corps K, y compris les points archimédiens.

Fixons un système de notations. Soit $X = X_{\mathrm{na}} \cup X_{\mathrm{a}}$, où X_{na} est constitué de tous les points non archimédiens de X, et X_{a}, de tous les points archimédiens.

Soit π un point de X. Le symbole K_π désignera le corps local correspondant. Si $f \in K$, le symbole f_π désignera le même élément f, considéré comme un élément du corps K_π. En outre,

(a) Si $\pi \in X_{\mathrm{na}}$, le symbole v_π désignera la valuation discrète standard du corps K_π, le symbole k_π, le corps résiduel de K_π. On pose aussi $\deg \pi = \log \operatorname{Card} k_\pi$.

(b) pour $\pi \in X_{\mathrm{a}}$ et $f \in K$ on pose

$$\varepsilon(\pi) = [K_\pi : \mathbb{R}] \ ;$$

$$\|f_\pi\| = |f_\pi|^{\varepsilon(\pi)}, \text{ où } |\cdot| \text{ est la valeur absolue usuelle} \ ;$$

$$v_\pi(f) = -\log \|f_\pi\| \ ;$$

$$\deg \pi = 1.$$

2.2. Que mettre à la place du corps des constantes. Les "constantes" dans K sont les éléments qui sont "entiers" en tous les points, y compris archimédiens. Si l'on considère que les entiers réels (complexes) sont les nombres dont le module est $\leqslant 1$, alors les "constantes" dans K sont 0 et les racines de l'unité. Dans ce qui suit, le symbole μ_N désignera l'ensemble des racines de l'unité de degré N (dans le corps $\overline{\mathbb{Q}}$), μ, la réunion de tous les μ_N. Le symbole $\mathbb{F}_N$ désignera l'ensemble constitué de 0 et des éléments de μ_N, $\mathbb{F}_\infty$, la réunion de tous les $\mathbb{F}_N$. Bien sûr, $\mathbb{F}_N$ et $\mathbb{F}_\infty$ ne sont pas des corps, mais nous nous efforcerons, dans la mesure du possible, de les traiter comme des corps et nous utiliserons même l'expression "corps" $\mathbb{F}_N$.

2.3. Que mettre à la place de $\mathbb{P}^1$. Tentons de définir à la main les points de $\mathbb{P}^1/\mathbb{F}_N$. Cela se fait en deux étapes.

Étape 1. D'abord, décrivons les "points géométriques" de $\mathbb{P}^1$, c'est-à-dire $\mathbb{P}^1(\mathbb{F}_\infty)$. Ce sont ∞, 0 et les points de la forme ε, où ε parcourt μ.

Étape 2. Décrivons les "points schématiques" de $\mathbb{P}^1/\mathbb{F}_N$. Le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_N))$ agit sur μ, et donc sur $\mathbb{P}^1(\mathbb{F}_\infty)$ (l'action de ce groupe sur 0 et ∞ est par définition triviale). On appellera "point schématique" les orbites de cette action. Le degré d'un tel point est par définition égal à la

longueur de l'orbite.

Comme on a affaire non seulement à des corps purement cyclotomiques, il convient de généraliser légèrement la construction précédente. À savoir, pour un sous-groupe arbitraire $\Gamma \subset \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q})$, le symbole $\mathbb{P}^1_1$ désignera l'ensemble constitué des orbites de l'action de Γ dans $\mathbb{P}^1(\mathbb{F}_\infty)$. Par convention, chaque point de $\mathbb{P}^1_1$ a un degré, la longueur de l'orbite.

Pour un corps quelconque K, on pose $\Gamma = \mathrm{Gal}(\mathbb{Q}(\mu)/L)$, où $L = K \cap \mathbb{Q}(\mu)$. Notons que L ne dépend pas du plongement choisi de K dans $\overline{\mathbb{Q}}$, car $K^\sigma \cap \mathbb{Q}(\mu) = (K \cap \mathbb{Q}(\mu))^\sigma = L^\sigma$. Et comme tous les sous-corps $\mathbb{Q}(\mu)$ sont normaux sur $\mathbb{Q}$, on a $L^\sigma = L$.

Ainsi, comme $\mathbb{P}^1$ nous prendrons désormais $\mathbb{P}^1_1$.

Remarque : le cas $K = \mathbb{Q}$ est particulièrement intéressant. Dans ce cas, les points de $\mathbb{P}^1_1$ seront notés ainsi : $\infty, 0, [1], [2], \ldots$, où le symbole $[d]$ désigne la "classe de points" constituée de toutes les racines primitives de l'unité de degré d. Son degré est $\deg[d] = \varphi(d)$, la fonction d'Euler.

2.4. Que signifie $f \neq$ const. Conformément à ce qui a été exposé ci-dessus (n° 2.2), partout dans ce qui suit nous supposerons que $f \neq 0$ et $f \notin \mu$.

Il y a encore un type de nombres que, pour certaines raisons (voir 2.5 (a)), nous excluons de l'examen.

Définition. Un nombre $f \in K$ est appelé exceptionnel s'il existe un point archimédien π tel que $\|f_\pi\| = 1$.

Notons qu'il existe des nombres exceptionnels qui ne sont pas des racines de l'unité (par exemple, $f = (3 + 4\sqrt{-1})/5$).

Dans ce qui suit, nous supposerons que f n'est pas exceptionnel.

2.5. Comment f définit une application $f : X \to \mathbb{P}^1_1$. Soit π un point de X. Considérons trois cas.

(a) $\pi \in X_{\mathrm{a}}$ (ou $\pi \in X_{\mathrm{na}}$ et $v_\pi(f) \neq 0$).

On pose

$$f(\pi) = \begin{cases} 0, & \text{si } v_\pi(f) > 0, \\ \infty, & \text{si } v_\pi(f) < 0. \end{cases}$$

Puisque f est supposé non exceptionnel, le cas $v_\pi(f) = 0$ pour $\pi \in X_{\mathrm{a}}$ ne peut pas se produire.

(b) $\pi \in X_{\mathrm{na}}$ et $v_\pi(f) = 0$. Soit $p = \mathit{chark}_\pi$. Le symbole Q désignera l'ensemble des racines $\varepsilon \in \mu$ satisfaisant aux conditions suivantes :

(i) l'ordre de ε est premier à p ;

(ii) il existe un idéal premier $\mathfrak{P}$, divisant π dans le corps $\mathbb{Q}(\varepsilon)$, pour lequel $f \equiv \varepsilon \pmod{\mathfrak{P}}$.

Lemme 1. *1. Q est une orbite de l'action de Γ dans μ.*

La démonstration s'obtient sans peine et est omise ici.

On pose $f(\pi) = Q$.

2.6. Qu'est-ce que $\deg f$**.** Par définition $\operatorname{div} f = \sum_{\pi \in X} v_\pi(f)[\pi]$. Ce diviseur se représente de manière unique comme la différence de deux diviseurs effectifs étrangers :

$$\operatorname{div} f = \operatorname{div}^+ f - \operatorname{div}^- f,$$

où

$$\operatorname{div}^+ f = \sum_{v_\pi(f)>0} v_\pi(f)[\pi], \quad \operatorname{div}^- f = -\sum_{v_\pi(f)<0} v_\pi(f)[\pi].$$

En vertu de la formule du produit d'Artin–Whittaker

$$\deg \operatorname{div}^+ f = \deg \operatorname{div}^- f.$$

On pose

$$\deg f = \deg \operatorname{div}^+ f.$$

2.7. Caractéristique d'Euler. On pose $\chi(X) = -\log|d_K| - r_2\gamma$, où d_K est le discriminant absolu de K ; r_2 est le nombre de points complexes de K ; γ est une certaine constante qui remplace $v_{\mathbb{C}}(D_{\mathbb{C}/\mathbb{R}})$. L'auteur ne connaît qu'une seule façon de normaliser γ. À savoir, si l'on considère que $\chi_{\text{top}} = 2\chi_{\text{hol}}$, alors d'après Szpiro (voir [2, 3]) on peut poser $\gamma = -2\log(\pi/2)$.

Pour formuler l'hypothèse principale, il ne reste plus qu'à définir le défaut. C'est le but du paragraphe suivant.

§ 3. Définition des défauts et formulation de l'hypothèse principale

Nous suivrons le principe suivant : nous ne pouvons définir que la partie modérée du défaut, et encore pas en tous les points de X. L'ensemble des points où le défaut est défini sera noté $X(f)$. Ce sont les points de X que f envoie sur des points "rationnels" de $\mathbb{P}^1_1$ (un point Q est "rationnel" si $\deg Q = 1$). Pour tenir compte des défauts en tous les points de X, on peut procéder de la manière suivante : d'abord, ajouter au corps K certaines racines de l'unité, puis réécrire les énoncés obtenus en termes de K. Cette méthode de définition des défauts est utilisée plus loin (voir n° 5.4) lors de la discussion des nombres premiers singuliers. Quant aux défauts totaux, l'auteur ne sait pas comment les définir. C'est l'une des principales lacunes de la théorie.

3.1. L'ensemble $X(f)$**.** Soit $X(f)$ l'ensemble des points $\pi \in X$ pour lesquels soit $v_\pi(f) > 0$, soit $v_\pi(f) < 0$, soit $v_\pi(f - \varepsilon) > 0$ pour un certain ε de $\mu \cap K$.

3.2. Les défauts modérés. Les défauts modérés sont définis par analogie avec la formule (1.4).

Soit π un point de X. Considérons plusieurs cas.

(a) $v_\pi(f) > 0$. On pose $\delta_\pi = \dfrac{[v_\pi(f) - 1] \deg \pi}{\deg f}$.

(b) $v_\pi(f) < 0$. On pose $\delta_\pi = \dfrac{[v_\pi(1/f) - 1] \deg \pi}{\deg f}$.

(c) $v_\pi(f - \varepsilon) > 0$, où $\varepsilon \in (\mu \cap K)$. Si $\pi \in X_{\mathrm{a}}$, le défaut δ_π est défini dans les cas (a) et (b). Nous supposerons que $\pi \in X_{\mathrm{na}}$.
Écrivons ε sous la forme $\varepsilon = \varepsilon_0 \varepsilon_1$, où l'ordre de ε_0 est premier à p ($p = c\mathit{hark}_\pi$), et l'ordre de ε_1 est une puissance de p. Rappelons que dans ce cas $f(\pi) = \varepsilon_0$ (voir 2.5 (b)). On pose $\delta_\pi = \dfrac{[v_\pi(f - \varepsilon_0) - 1] \deg \pi}{\deg f}$.

Remarque : il semble important d'utiliser autant que possible uniquement les propriétés multiplicatives des nombres. Dans la définition du défaut δ_π dans le cas (c), il y a une expression additive $(f - \varepsilon_0)$, mais en réalité l'ordre de cette quantité reflète le degré de précision de l'égalité $f = \varepsilon_0$ et, par conséquent, est déterminé par les propriétés multiplicatives de f.

3.3. Ramification sauvage en un point archimédien. Avant de formuler l'hypothèse principale, discutons d'un effet lié à la ramification sauvage en un point archimédien. Par analogie avec le cas fonctionnel, l'"ordre de la dérivée" d'un nombre réel x par rapport au "paramètre local" du corps $\mathbb{R}$ sera cherché sous la forme

$$v(x') = v(x) - 1 + s(x),$$

où la fonction $s(x)$ décrit la partie sauvage de la "dérivée". Pour une raison qui apparaîtra clairement ci-dessous, nous aurons affaire à la fonction $R_1(x) = -s(x)$. Nous supposerons que nous ne connaissons pas cette fonction, mais nous formulerons seulement une série de conditions pour elle :

(a) $R_1(x)$ est définie et continue dans $\mathbb{R}^*$;

(b) $R_1(x) = R_1(-x) = R_1(1/x)$;

(c) $R_1(x) = o(\log x)$ lorsque $x \to +\infty$.

Dans la version initiale du travail, une hypothèse plus forte sur l'asymptotique de la fonction $R_1(x)$ avait été faite, à savoir :

$$R_1(x) \sim \log \log x \quad \text{lorsque } x \to +\infty.$$

Cette hypothèse avait été faite à partir des considérations heuristiques exposées ci-dessous.

Pour $x \in \mathbb{R}^*$, la formule suivante est valable :

$$x = \int_{-\log|x|}^{\infty} \mathrm{sign}(x)(1/e)^s ds.$$

Cette formule peut être considérée comme un analogue du développement d'une fonction en série de Laurent. Si $f \in k((t))$, alors

$$f = \sum_{v_i(f)}^{\infty} a_n t^n.$$

L'analogue formel de la dérivée par rapport au paramètre local sera l'expression

$$x' = \int_{-\log|x|}^{\infty} \mathrm{sign}(x) s (1/e)^{s-1} ds.$$

Pour $0 < |x| < 1$ nous obtenons

$$x' = \mathrm{sign}(x) e |x| (1 + \log(1/|x|))$$

et

$$v(x') = -\log|x| - 1 - \log(1 + \log(1/|x|)).$$

Partant de là, il faudrait poser

$$s(x) = -\log(1 + \log(1/|x|)), \tag{3.1}$$

ce qui donne l'asymptotique $R_1(x) \sim \log\log x$ lorsque $x \to +\infty$. Cette hypothèse sur l'asymptotique de la fonction $R_1(x)$ était apparemment confirmée par les exemples 1–5 (voir § 4). Cependant, A. N. Parshin a signalé à l'auteur le travail de Masser [5], duquel il résulte qu'au moins $R_1(x) = O(\sqrt{\log x})$ (voir n° 6, § 4). C'est pourquoi nous nous limitons pour l'instant à l'hypothèse (c) : $R_1(x) = o(\log x)$.

Notons que si l'on définit la fonction $s(x)$ par la formule (3.1), alors la partie sauvage de la dérivée sera négative (contrairement au cas fonctionnel). Un effet semblable peut être observé dans la définition de $\chi(X)$ si l'on choisit la normalisation de Szpiro (voir n° 2.7). Le terme $2r_2 \log(\pi/2)$ est positif, alors que dans le cas fonctionnel toute ramification rend la caractéristique d'Euler plus négative. De cette discussion, il ressort que dans l'inégalité de Hurwitz on ne peut, en général, ignorer la ramification sauvage aux points archimédiens, car elle peut être négative. Pour cette même raison, nous travaillons avec la fonction $R_1(x) = -s(x)$ au lieu de la fonction $s(x)$.

Considérons maintenant le cas complexe. Soit $z \in \mathbb{C}$. Nous chercherons $v_{\mathbb{C}}(z')$ sous la forme

$$v_{\mathbb{C}}(z') = v_{\mathbb{C}}(z) - 1 - R_2(z),$$

où $R_2(z)$ est une fonction inconnue. Il est naturel de considérer que R_2 dépend seulement du module de z. Il suffit donc de définir $R_2(x)$ pour $x \in \mathbb{R}$. Si l'on part de l'analogie avec le cas fonctionnel, on doit considérer que

$$v_{\mathbb{C}}(x') = 2v_{\mathbb{R}}(x') + v_{\mathbb{C}}(D_{\mathbb{C}/\mathbb{R}}).$$

Dans la définition de $\chi(X)$ (voir n° 2.7) apparaissait la constante γ, qui remplace $v_{\mathbb{C}}(D_{\mathbb{C}/\mathbb{R}})$. En passant aux fonctions R_1 et R_2, on obtient

$$v_{\mathbb{C}}(x) - 1 - R_2(x) = 2v_{\mathbb{R}}(x) - 2 - 2R_1(x) + \gamma.$$

Compte tenu de ce que $v_{\mathbb{C}}(x) = 2v_{\mathbb{R}}(x)$, on obtient

$$R_2(x) = 2R_1(x) + 1 - \gamma.$$

Ainsi, posons $R_2(z) = 2R_1(|z|) + 1 - \gamma$.

3.4. L'hypothèse principale. Nous sommes maintenant prêts à formuler l'hypothèse principale, que nous appellerons hypothèse A.

Hypothèse A : il existe une fonction $R_1(x)$ satisfaisant aux conditions (a), (b), (c) (voir 3.3), telle que pour un corps de nombres K arbitraire et tout $f \in K$ non exceptionnel (voir 2.4) l'inégalité suivante soit vraie :

$$\sum_{\pi \in X(f)} \delta_\pi \leq 2 - \frac{\chi(K)}{\deg f} + \sum_{\pi \in X_{\mathrm{a}}} \frac{R_\pi(f_\pi)}{\deg f}.$$

3.5. Un affaiblissement de l'hypothèse principale. L'hypothèse A suppose la possibilité de faire varier le corps de base K. Ci-dessous nous donnons un affaiblissement de celle-ci, dans lequel le corps K est fixé. De plus, nous fixons un $\epsilon > 0$ arbitraire.

Hypothèse $B(K)$: il existe une constante $C = C(\epsilon, K)$ telle que pour tout $f \in K^*$ non exceptionnel l'inégalité suivante soit vraie :

$$\sum_{\pi \in X(f)} \delta_\pi \leq 2 + \epsilon + \frac{C}{\deg f}.$$

3.6. Le cas $K = \mathbb{Q}$**.** Dans ce cas, le "corps des constantes" (voir 2.2) coïncide avec $\mathbb{F}_2$ et $\mathbb{P}^1/\mathbb{F}_2$ possède 4 points "rationnels", ∞, 0, $[1] = \{1\}$ et $[2] = \{-1\}$. Rappelons que pour $Q \in \mathbb{P}^1$ le défaut $\delta_Q = \sum_{\pi \to Q} \delta_\pi$.

Fixons le système de notations suivant : pour un entier naturel $A = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ on pose

$$A_0 = p_1 \dots p_r, \text{ la partie sans facteur carré de } A;$$

$$A_1 = A/A_0, \text{ tout le reste.}$$

Soit $f = m/n \in \mathbb{Q}$. Nous supposerons que $m > n > 0$ et $(m, n) = 1$. Dans ce cas $\deg f = \log m$. En comparant avec la définition (voir n° 3.2), nous obtenons

$$\left.\begin{aligned} \delta_0 &= \frac{\log m_1}{\log m}, \\ \delta_\infty &= \frac{\log n_1 + \log(m/n) - 1}{\log m}, \\ \delta_1 &= \frac{\log(m-n)_1}{\log m}, \\ \delta_2 &= \frac{\log k_1}{\log m}, \quad \text{où } k = (m+n)/2^{v_2(m+n)}. \end{aligned}\right\} \tag{3.3}$$

Ici $\delta_0, \delta_\infty, \delta_1, \delta_2$ sont les défauts aux points 0, ∞, [1] et [2] respectivement.

L'hypothèse $B(K)$ dans le cas $K = \mathbb{Q}$ se réduit donc à l'énoncé suivant $B(\mathbb{Q})$.

Pour tout $\epsilon > 0$ il existe une constante $C(\epsilon)$ telle que pour toute paire $m > n > 0$ avec $(m, n) = 1$ l'inégalité suivante soit vraie

$$\delta_\infty + \delta_0 + \delta_1 + \delta_2 \le 2 + \epsilon + \frac{C(\epsilon)}{\log m}. \qquad B(\mathbb{Q})$$

§ 4. Quelques exemples

Dans ce paragraphe, nous nous intéresserons au cas $K = \mathbb{Q}$. On construit cinq séries différentes d'exemples montrant la précision asymptotique de l'inégalité $B(\mathbb{Q})$. En outre, dans le contexte de ce travail, on donne un résultat de Stewart et Tijdeman (voir [4, 5]), qui donne la meilleure estimation connue de l'auteur pour la fonction $R_1(x)$ par défaut.

Le symbole const désignera les nombreuses constantes apparaissant au cours du travail. Ces constantes peuvent dépendre de certains paramètres, c'est pourquoi dans les formulations des propositions on indique les quantités dont ces constantes ne dépendent pas.

4.1. Tore G_m (1 + 1 + 0 + 0). Fixons une paire d'entiers naturels a et b. Nous supposerons que $a > b > 1$ et $(a, b) = 1$.

Proposition 2. *1. Il existe une infinité de paires d'entiers naturels (r, s) telles que*

$$\delta_\infty + \delta_0 + \delta_1 + \delta_2 \ge 2 + \frac{\log\log m}{\log m} - \frac{\text{const}}{\log m},$$

où $m = a^r$, $n = a^r - b^s$; les défauts sont liés au nombre $f = m/n$. Toutes les constantes ne dépendent pas de r et s.

Démonstration. Prenons comme s/r les fractions convergentes de $\log a/\log b$ qui approchent par la gauche. Alors, d'après l'estimation standard de la théorie des fractions convergentes, l'inégalité suivante est vraie :

$$0 < \frac{\log a}{\log b} - \frac{s}{r} < \frac{1}{r^2}. \tag{4.1}$$

Commençons à estimer les défauts.

$$\text{(a)} \quad \delta_0 = \frac{\log m_1}{\log m} \ge \frac{\log a^{r-1}}{\log m} = 1 - \frac{\log a}{\log m} \ge 1 - \frac{\text{const}}{\log m}.$$

$$\text{(b)} \quad \delta_\infty \ge \frac{\log m - \log n - 1}{\log m}. \tag{4.2}$$

De l'estimation (4.1) il résulte que

$$s\log b < r\log a < s\log b + \log b/r.$$

Par conséquent,

$$0 < a^r - b^s < b^s(b^{1/r} - 1). \tag{4.3}$$

En développant $(b^{1/r} - 1)$ en série en puissances de $\log b/r$, nous voyons que pour tout $\varepsilon > 0$ et r suffisamment grand l'inégalité suivante est vraie :

$$n \le \frac{b^s(1+\varepsilon)\log b}{r}.$$

Par conséquent,

$$n \le \frac{a^r(1+\varepsilon)\log b \log a}{\log m}. \tag{4.4}$$

En combinant les estimations (4.2) et (4.4), nous voyons que

$$\delta_\infty \ge \frac{\log\log m}{\log m} - \frac{1+\log(1+\varepsilon)+\log\log a+\log\log b}{\log m} \ge \frac{\log\log m}{\log m} - \frac{\text{const}}{\log m},$$

$$\text{(c)} \quad \delta_1 \ge \frac{s\log b - \log b}{\log m} \ge \frac{s\log b}{\log m} - \frac{\text{const}}{\log m}.$$

Compte tenu de (4.3), nous obtenons

$$\delta_1 \ge \frac{\log a^r - (\log b)/r}{\log m} - \frac{\text{const}}{\log m} \ge 1 - \frac{\text{const}}{\log m}.$$

$$\text{(d)} \quad \delta_2 \ge 0.$$

En combinant les estimations (a), (b), (c) et (d), nous obtenons la démonstration de la proposition.

Remarque : le type de tous les exemples, dans ce cas $(1+1+0+0)$, est lié à l'estimation inférieure des quatre défauts. La somme des quatre nombres entre parenthèses est toujours égale à 2, et ce même 2 est le terme dominant dans le membre de droite de l'inégalité de Hurwitz.

4.2. Triplets pythagoriciens (3/4 + 3/4 + 1/2 + 0). Soit $a^2+b^2=c^2$, où a, b, c sont des entiers naturels deux à deux premiers entre eux.

Proposition 3. *2. Il existe une infinité de triplets pythagoriciens (a, b, c) tels que*

$$\delta_\infty + \delta_0 + \delta_1 + \delta_2 \ge 2 + \frac{\log\log m}{\log m} - \frac{\text{const}}{\log m},$$

où $m = c^2$, $n = a^2$, $f = m/n$, toutes les constantes ne dépendent pas de m et n.

Démonstration. Nous chercherons les triplets (a, b, c) sous la forme standard : $a = 2xy$, $b = x^2 - y^2$, $c = x^2 + y^2$. Posons $x = 2^r$, $y = 2^r - 1$, où $r = 2 \cdot 3^\alpha$; $\alpha = 1, 2, \ldots$

$$\text{(a)} \quad \delta_0 \ge \frac{\log(c^2)_1}{\log c^2} \ge \frac{1}{2}.$$

$$\text{(b)} \quad \delta_\infty \ge 1 - \frac{\log b + 1}{\log m} \ge 1 - \frac{(r+1)\log 2 + \log(1 - 1/2^{r+1})}{\log m} - \frac{\text{const}}{\log m}. \tag{4.5}$$

Estimons r par m.

$$m = c^2 = 2^{4r+2}(1 - 1/2^{r+1} + 1/2^{2r+1}).$$

En posant $\varepsilon = 1/2^{r+1} - 1/2^{2r+1}$, nous obtenons

$$\log m \le (4r+2)\log 2 \le \log m - 2\log(1-\varepsilon) \le \log m + 2\varepsilon \log 2.$$

Par conséquent,

$$\frac{\log m}{4\log 2} - \frac{1}{2} \le r \le \frac{\log m}{4\log 2} - \frac{1}{2} + \frac{\varepsilon}{2}.$$

En substituant cette estimation dans (4.5), nous obtenons

$$\delta_\infty \ge 1 - \frac{[\log m/(4\log 2) - 1/2 + \varepsilon/2]\log 2}{\log m} - \frac{\text{const}}{\log m} \ge \frac{3}{4} - \frac{\text{const}}{\log m}.$$

$$\text{(c)} \quad \delta_1 = \frac{\log[2^{2r+2}3^{2\alpha+2}(2^r-1)/3^{\alpha+1}]_1}{\log m}. \tag{4.6}$$

Comme $r = 2\cdot 3^\alpha$, alors $2^r \equiv 1 \pmod{3^{\alpha+1}}$. Par conséquent (4.6) entraîne

$$\delta_1 \ge \frac{(2r+1)\log 2 + (2\alpha+1)\log 3 + \log[(2^r-1)/3^{\alpha+1}]}{\log m} =$$

$$= \frac{(2r+1)\log 2 + \alpha\log 3 + r\log 2 + \log(1-1/2^r)}{\log m} \ge$$

$$\ge \frac{(\log m)/2 + (\log r/\log 2 - \log 2/\log 3)\log 3 + r\log 2 - \log 2}{\log m} =$$

$$= \frac{1}{2} + \frac{\log r}{\log m} + \frac{1}{4} - \frac{\text{const}}{\log m} \ge \frac{3}{4} + \frac{\log\log m}{\log m} - \frac{\text{const}}{\log m}.$$

En additionnant les estimations (a), (b), (c), nous obtenons la démonstration de la proposition 2.

4.3. Cubique de Fermat (2/3 + 2/3 + 2/3 + 0). Considérons la courbe elliptique E, donnée par l'équation $AX^3 + AY^3 = BZ^3$, où A et B sont des entiers naturels deux à deux premiers entre eux, sans facteurs cubiques. Comme origine sur E prenons le point $P_0 = (1:-1:0)$. Supposons que sur E il y a un point P_1 d'ordre infini. Soit $P_r = rP_1$ et (x_r, y_r, z_r) les coordonnées du point P_r, choisies de telle sorte que $x_r > 0$ et $(x_r, y_r, z_r) = 1$. Exemple d'une telle situation : $A = 1, B = 9, P_1 = (2:1:1)$.

Proposition 4. *3. Il existe une infinité de valeurs de r telles que*

$$\delta_\infty + \delta_0 + \delta_1 + \delta_2 \ge 2 + \frac{1}{2}\frac{\log\log m}{\log m} - \frac{\text{const}}{\log m},$$

où $m = Bz_r^3$, $n = Ay_r^3$, $f = m/n$; toutes les constantes ne dépendent pas de r.

Démonstration. Apparemment, le fait suivant est bien connu, mais l'auteur n'a pas réussi à trouver une référence appropriée.

Lemme 5. *1. Soient $\alpha, \xi \in \mathbb{R}/\mathbb{Z}$, ξ irrationnel. Alors il existe une infinité de r tels que*

$$0 < r\xi - \alpha < \frac{2}{r}$$

(pour les points voisins sur le cercle, la relation $<$ a un sens).

La démonstration du lemme 1, utilisant par exemple les propriétés des fractions convergentes, s'obtient facilement et n'est pas donnée ici.

Lemme 6. *2. Il existe une constante positive λ telle que pour une infinité de r l'inégalité suivante soit vraie :*

$$0 < y_r < \lambda z_r / r.$$

Démonstration du lemme 2. Soit ω une différentielle invariante sur E, définie sur $\mathbb{R}$. En appliquant le lemme 1 au cercle $E(\mathbb{R})$, muni de la métrique induite par ω, nous voyons qu'il existe une constante λ_0 telle que pour une infinité de r les conditions suivantes soient satisfaites : $y_r > 0$ et la distance du point P_r au point $Q = (\sqrt[3]{B} : 0 : \sqrt[3]{A})$, mesurée à l'aide de ω, ne dépasse pas λ_0/r. Comme la tangente à E au point Q n'est pas parallèle à l'axe des x, les distances au voisinage de Q sont uniformément estimées par la différence des coordonnées y. Cela démontre le lemme 2.

Poursuivons la démonstration de la proposition 3. Comme A et B sont sans facteurs cubiques, $m = Bz_r^3$ et $n = Ay_r^3$ sont premiers entre eux. Nous considérerons les valeurs de r satisfaisant à l'inégalité du lemme 2, et commencerons à estimer les défauts.

$$\text{(a)} \quad \delta_0 \geq \frac{\log z_r^2}{\log m} = \frac{2}{3} - \frac{2\log B}{3\log m};$$

$$\text{(b)} \quad \delta_\infty \geq \frac{2\log y_r + \log(m/n) - 1}{\log m} \geq 1 - \frac{\log y_r}{\log m} - \frac{\text{const}}{\log m}.$$

D'après le choix de r, l'inégalité $y_r \leq \text{const} \cdot z_r/r$ est vraie. Par conséquent,

$$\begin{aligned} \delta_\infty &\geq 1 - \frac{\log z_r - \log r}{\log m} - \frac{\text{const}}{\log m} \geq \\ &\geq 1 - \frac{1}{3}\frac{\log Bz_r^3}{\log m} + \frac{\log r}{\log m} - \frac{\text{const}}{\log m}. \end{aligned} \tag{4.8}$$

Notons que $\log z_r$ est la hauteur logarithmique du point P_r et, par conséquent, $\log z_r = \text{const} r^2(1 + o(1))$. Donc (4.8) entraîne l'estimation

$$\delta_\infty \geq \frac{2}{3} + \frac{1}{2}\frac{\log\log m}{\log m} - \frac{\text{const}}{\log m};$$

$$\text{(c)} \quad \delta_1 \geq \frac{2\log x_r}{\log m} \geq \frac{2\log(m - \text{const} z_r^3/r)}{\log m} - \frac{\text{const}}{\log m} \geq \frac{2}{3} + \frac{\log(1 - \text{const}/(Br^3))}{\log m} - \frac{\text{const}}{\log m} \geq \frac{2}{3} - \frac{\text{const}}{\log m}.$$

En combinant les estimations (a), (b) et (c), nous obtenons la démonstration de la proposition 3.

4.4. Quartique de Jacobi (3/4 + 3/4 + 1/2 + 0). Considérons la courbe elliptique E donnée par l'équation $AY^2Z^2 = B(X^4 - Z^4)$, avec pour origine $P_0 = (1 : 0 : 1)$. Supposons que sur E il y a un point P_1 d'ordre infini. Soit $P_r = rP_1$ de coordonnées $(x_r : y_r : z_r)$.

Proposition 7. *4. Il existe une infinité de valeurs de r telles que*

$$\delta_\infty + \delta_0 + \delta_1 + \delta_2 \geq 2 + \frac{1}{2}\frac{\log\log m}{\log m} - \frac{\text{const}}{\log m},$$

où $f = Bx_1^4/(Ay_1^2z_1^2)$, m est le numérateur de f, n le dénominateur de f ; const *ne dépend pas de r.*

La proposition 4 se démontre par la même méthode que la proposition 3.

4.5. Paire de quadriques sous la forme de Mumford (1/2 + 1/2 + 1/2 + 1/2). Considérons la courbe elliptique E donnée par une paire de quadriques dans $\mathbb{P}^3$ (voir [6]).

$$\begin{cases} A(X^2+Y^2) = BZ^2, \\ C(X^2-Y^2) = DT^2. \end{cases}$$

Supposons que sur E soit marqué un zéro P_0 et qu'il y ait un point P_1 d'ordre infini. Soit le point $P_r = rP_1$ de coordonnées x_r, y_r, z_r, t_r.

Proposition 8. *5. Il existe une infinité de valeurs de r telles que*

$$\delta_\infty + \delta_0 + \delta_1 + \delta_2 \geq 2 + \frac{1}{2}\frac{\log\log m}{\log m} - \frac{\text{const}}{\log m},$$

où $f = x_r^2/y_r^2$, m est le numérateur de f, n le dénominateur de f ; const *ne dépend pas de r.*

La proposition 5 se démontre par la même méthode que la proposition 3.

4.6. L'exemple de Stewart et Tijdeman. Dans le travail [4] (voir aussi [5]), pour tout $\delta > 0$ on a construit une série de triplets d'entiers (a, b, c) tels que

(a) $a + b + c = 0$, a, b, c sont deux à deux premiers entre eux ;

(b) $\max(|a|, |b|, |c|) \geqslant S \exp\{(4-\delta)(\log S)^{1/2}(\log\log S)^{-1}\}$,

où $S = |abc|_0$.

Comme on le voit facilement, de ce résultat découle la proposition suivante.

Proposition 9. *6. Pour tout $\epsilon > 0$ et $\delta > 0$ il existe une infinité de paires d'entiers naturels premiers entre eux m et n tels que*

$$\delta_\infty + \delta_0 + \delta_1 + \delta_2 \geq 2 + (4-\delta)\frac{(\log m)^{1/2-\epsilon}}{\log m} - \frac{\text{const}}{\log m},$$

où const *ne dépend pas de m et n.*

Pour la démonstration, il suffit d'utiliser le résultat ci-dessus en posant $m = \max(|a|, |b|, |c|)$, $n = \min(|a|, |b|, |c|)$.

§ 5. Applications de l'inégalité de Hurwitz

Dans ce paragraphe, on donne quelques conséquences de l'hypothèse principale. Premièrement, c'est la célèbre conjecture ABC de Masser et Oesterlé. On sait (voir, par exemple, [8]) que la conjecture ABC entraîne plusieurs résultats diophantiens intéressants : le théorème de Fermat asymptotique, l'inégalité de Szpiro, etc. Nous montrons que de l'inégalité de Hurwitz découle une version plus forte de l'inégalité de Szpiro, proposée par Parshin (voir [7]). Cette version tient compte des composantes

archimédiennes de la hauteur des courbes elliptiques. Ensuite, l'hypothèse $B(\mathbb{Q})$ est appliquée pour estimer l'ordre d'approximation des logarithmes par des nombres rationnels. Cette estimation est comparée aux résultats de Feldman et Waldschmidt. Après cela, nous passons à l'étude des nombres premiers singuliers, c'est-à-dire ceux p pour lesquels $f^p \equiv f \pmod{p^2}$ (le nombre rationnel f est ici fixé). De tels nombres apparaissent de temps en temps dans des problèmes de théorie des nombres, cependant leur étude se heurte à des difficultés considérables. L'application de l'hypothèse principale sous sa forme forte, l'hypothèse A, permet d'obtenir des estimations intéressantes sur la croissance de ces nombres.

Comme ci-dessus, le symbole const désignera toutes les constantes possibles apparaissant au cours du travail.

5.1. La conjecture ABC.

Théorème 10. *1.*

De l'hypothèse $B(\mathbb{Q})$ découle la conjecture ABC suivante : pour tout $\varepsilon > 0$ il existe une constante const *(dépendant seulement de ε) telle que pour toute paire d'entiers naturels premiers entre eux A et B l'inégalité suivante soit satisfaite :*

$$C \le \mathrm{const}(A_0 B_0 C_0)^{1+\varepsilon},$$

où $C = A + B$.

Démonstration. Posons $m = C$, $n = \min(A, B)$ et estimons les défauts.

$$\text{(a)} \quad \delta_0 = \frac{\log m_1}{\log m} = 1 - \frac{\log m_0}{\log m};$$

$$\text{(b)} \quad \delta_\infty = \frac{\log n_1 + \log(m/n) - 1}{\log m} \ge 1 - \frac{\log n_0}{\log m} - \frac{\mathrm{const}}{\log m};$$

$$\text{(c)} \quad \delta_1 = \frac{\log(m-n)_1}{\log m} = \frac{\log(m-n)}{\log m} - \frac{\log(m-n)_0}{\log m}.$$

Comme $n = \min(A, B)$, on a $m - n \ge m/2$ et, par conséquent,

$$\delta_1 \ge 1 - \frac{\log(m-n)_0}{\log m} - \frac{\mathrm{const}}{\log m}.$$

$$\text{(d)} \quad \delta_2 \ge 0.$$

En appliquant l'inégalité $B(\mathbb{Q})$, nous obtenons

$$3 - \frac{\log(m_0 n_0 (m-n)_0)}{\log m} \le 2 + \varepsilon + \frac{\mathrm{const}}{\log m}.$$

Il en résulte que

$$(1-\varepsilon)\log m \le \log(m_0 n_0 (m-n)_0) + \mathrm{const}$$

et, par conséquent,

$$m^{1-\varepsilon} \leq \text{const}(m_0 n_0 (m-n)_0).$$

D'où l'inégalité

$$m \leq \text{const}(m_0 n_0 (m-n)_0)^{1+\varepsilon},$$

ce qu'il fallait démontrer.

5.2. L'inégalité de Szpiro (sous la forme de Parshin). Toutes les informations nécessaires sur les courbes elliptiques peuvent être trouvées dans les travaux [9] et [10].

Donnons la définition de la hauteur géométrique d'une courbe elliptique E définie sur un corps K :

$$h(E) = \sum_{\pi \in X_{\text{na}}} \log^+ \|j_\pi\| + 6 \sum_{\pi \in X_{\text{na}}} \log \|1/V(j_\pi)\|. \tag{5.1}$$

Ici $\log^+(x) = \max(0, \log x)$, j est le j-invariant de E, $V(j)$ est la fonction du travail [10] (voir aussi ci-dessous). Cette hauteur est 12 fois plus grande que la hauteur utilisée dans [10].

Théorème 11. *2. De l'hypothèse $B(\mathbb{Q})$ il découle que pour tout $\varepsilon > 0$ il existe une constante* const *(dépendant seulement de ε) telle que pour toute courbe elliptique stable E sur $\mathbb{Q}$ l'inégalité suivante soit vraie :*

$$h(E) \leq (6+\varepsilon) \log N + \text{const},$$

où N est le conducteur de E.

Démonstration. Soit Δ le discriminant minimal de E. En vertu de la stabilité $N = \Delta_0$. Soit $j = j(E)$, $J = j/1728$. Écrivons J sous la forme $J = \pm A/B$, où A et B sont des entiers naturels premiers entre eux. Notons que $J \neq \pm 1$, car de telles courbes ne peuvent pas être stables sur $\mathbb{Q}$. Posons $C = |A - B|$.

Lemme 12. *1.*

(i) $\log B + \text{const} \leq \log \Delta \leq \log B + \text{const}$, $\log B_0 + \text{const} \leq \log \Delta_0 \leq \log B_0 + \text{const}$;

(ii) $\log A_1 \geq \dfrac{2}{3} \log A - \text{const}$;

(iii) $\log C_1 \geq \dfrac{1}{2} \log C - \text{const}$.

Démonstration du lemme 1. En vertu de la stabilité de E, l'égalité $v_p(\Delta) = \max(0, -v_p(j))$ est satisfaite et, par conséquent, $B = \lambda \Delta$, où λ divise 1728. Cela démontre (i).

Ensuite, notons que pour $p \neq 2, 3$ les valeurs de $v_p(\Delta)$ sont multiples de 3, car il existe c_4 et c_6 tels que $j = c_4^3/(c_4^3 - c_6^2)$ et $\min(v_p(c_4), v_p(c_6)) = 0$ (voir [9]). Ainsi, $A = 2^\alpha 3^\beta a^3$. Alors $A_1 \geq 2^{\alpha-1} 3^{\beta-1} a^2 \geq \dfrac{1}{6} A^{2/3}$. Cela démontre (ii).

(iii) se démontre de façon analogue à (ii), en tenant compte du fait que pour $p \neq 2, 3$ la valeur de $v_p(\Delta)$ est multiple de 2. Le lemme 1 est démontré.

Lemme 13. *2. Pour $j \in \mathbb{C}$:* $6 \log(1/V(j)) \leq \log^+ |j| - 6 \log^+ \log^+ |j| + \text{const}$.

Démonstration du lemme 2. Toutes les notations sont tirées de [10].

$$V(j) = 4\pi y \left| q^{1/12} \prod_{n=1}^{\infty} (1-q^n) \right|^2, \tag{5.2}$$

où $q = \exp(2\pi i\tau)$, $y = \operatorname{Im}\tau > 0$, $j = j(q)$.

Notons que la fonction $V(j)$ est positive et séparée de 0, car on peut se limiter à considérer une figure modulaire, et là cela se voit à partir de (5.2). Par conséquent, la quantité $\log(1/V(j))$ est bornée dans les domaines bornés de $\mathbb{C}$, et il reste à examiner le comportement de $V(j)$ lorsque $y \to +\infty$. De (5.2) on voit que $\log(1/V(j)) \sim \dfrac{1}{6}\log(1/|q|) - \log y$. En tenant compte du fait que $y = \log|q|/2\pi$, et que le développement de j à l'infini commence ainsi : $j = 1/q + \ldots$, nous obtenons l'assertion du lemme 2.

Dans la démonstration du théorème 2, nous distinguerons plusieurs cas : 1) $A < C < B$; 2) $C < A < B$; 3) $B < C < A$; 4) $C < B < A$. De la définition de C on voit que les cas $A < B < C$ et $B < A < C$ ne se rencontrent pas.

Cas 1. $A < C < B$. Posons $f = B/A$. Notons que dans ce cas $A + C = B$ et, par conséquent, $C \geq B/2$.

$$\text{(a)} \quad \delta_0 = 1 - \frac{\log B_0}{\log B}.$$

$$\text{(b)} \quad \delta_\infty = \frac{\log A_1 + \log(B/A) - 1}{\log B}.$$

Compte tenu du point (ii) du lemme 1 (voir ci-dessus), nous obtenons

$$\delta_\infty \geq \frac{\frac{2}{3}\log A + \log(B/A) - 1}{\log B} \geq \frac{2}{3} - \frac{\text{const}}{\log B}.$$

$$\text{(c)} \quad \delta_1 = \frac{\log C_1}{\log B}.$$

Compte tenu du point (iii) du lemme 1, nous voyons que

$$\delta_1 \geq \frac{1}{2}\frac{\log C - \text{const}}{\log B} \geq \frac{1}{2}\frac{\log(B/2) - \text{const}}{\log B} \geq \frac{1}{2} - \frac{\text{const}}{\log B}.$$

$$\text{(d)} \quad \delta_2 \geq 0.$$

En appliquant l'inégalité $B(\mathbb{Q})$, nous obtenons

$$\left(\frac{1}{6} - \varepsilon\right)\log B \leq \log B_0 + C(\varepsilon).$$

Compte tenu du point (i) du lemme 1, nous voyons que

$$\log\Delta \leq (6+\varepsilon)\log N + \text{const}.$$

Comme dans le cas 1 la quantité $|j| = 1728A/B$ est bornée, par le lemme 2 la différence $(h(E) - \log \Delta)$ est aussi bornée. Par conséquent,

$$h(E) \leq (6 + \varepsilon) \log N + \text{const}.$$

Cas 2. $C < A < B$. Posons $f = B/C$. Notons que dans ce cas $A + C = B$ et, par conséquent, $A \geq B/2$.

$$\text{(a)} \quad \delta_0 = 1 - \frac{\log B_0}{\log B}.$$
$$\text{(b)} \quad \delta_\infty = \frac{\log C_1 + \log(B/C) - 1}{\log B}.$$

Compte tenu du point (iii) du lemme 1, nous obtenons

$$\delta_\infty \geq \frac{\log B - \frac{1}{2}\log C - 1}{\log B} \geq \frac{1}{2} - \frac{\text{const}}{\log B}.$$

$$\text{(c)} \quad \delta_1 = \frac{\log A_1}{\log B}.$$

Compte tenu du point (ii) du lemme 1, nous obtenons

$$\delta_1 \geq \frac{\frac{2}{3}\log A - \text{const}}{\log B} \geq \frac{\frac{2}{3}\log(B/2) - \text{const}}{\log B} \geq \frac{2}{3} - \frac{\text{const}}{\log B}.$$

Ensuite, la démonstration se fait parallèlement au cas 1.

Cas 3. $B < C < A$.

Posons $f = A/B$. Notons que dans ce cas $B + C = A$ et, par conséquent, $C \geq A/2$.

Compte tenu du lemme 1, nous obtenons les estimations suivantes des défauts :

$$\text{(a)} \quad \delta_0 \geq \frac{2}{3} - \frac{\text{const}}{\log A};$$
$$\text{(b)} \quad \delta_\infty \geq 1 - \frac{\log B_0}{\log A} - \frac{\text{const}}{\log A};$$
$$\text{(c)} \quad \delta_1 \geq \frac{1}{2} - \frac{\text{const}}{\log A};$$
$$\text{(d)} \quad \delta_2 \geq 0.$$

En appliquant l'inégalité $B(\mathbb{Q})$, nous obtenons

$$\log A \leq (6 + \varepsilon) \log B_0 + \text{const}. \tag{5.3}$$

Estimons la hauteur logarithmique de la courbe E :

$$h(E) = \log |\Delta| + 6 \log(1/V(j)).$$

Compte tenu du point (i) du lemme 1, nous voyons que

$$h(E) \leq \log B + 6 \log(1/V(\pm 1728A/B)).$$

En prenant en compte le lemme 2, nous obtenons

$$h(E) \leq \log B + \log(1728A/B) \leq \log A + \text{const}.$$

En combinant cette estimation avec (5.3), nous obtenons

$$h(E) \leq (6 + \varepsilon) \log N + \text{const}.$$

Cas 4. $C < B < A$.

Posons $f = A/C$. Notons que dans ce cas $C + B = A$ et $B \geq A/2$. La démonstration dans le cas 4 se fait parallèlement à celle du cas 3. Le théorème 2 est démontré.

Remarque : la même méthode permet de démontrer le théorème 2 dans le cas où le j-invariant est dans $\mathbb{Q}$ ou dans un corps quadratique imaginaire, et où la courbe est stable sur un corps K suffisamment grand (avec des constantes dépendant de K). Cependant, dans d'autres cas, cette méthode ne fonctionne pas, car selon le comportement de j au point archimédien, l'hypothèse était appliquée à différents f. Si le nombre de points archimédiens est supérieur à 1, cela ne passe plus.

5.3. Approximation des logarithmes. Soient $m > n > 0$ des entiers. Nous nous intéresserons à l'estimation inférieure de la quantité Λ, où

$$\Lambda = |a \log m - b \log n|.$$

Ici a et b sont des entiers naturels. Nous supposerons aussi que $a < b$ (seul ce cas est intéressant).

Des questions de ce genre ont été beaucoup étudiées. Donnons ici l'estimation de Feldman (voir [11], p. 154) : si $\log m$ et $\log n$ sont linéairement indépendants sur $\mathbb{Q}$, alors il existe une constante $C(m, n)$ telle que

$$\Lambda > b^{-C(m,n)}.$$

D'après le travail de Waldschmidt [12], on peut prendre $C(m, n) = \text{const} \cdot \log^2 m$, où const est une constante absolue.

Montrons que l'hypothèse $B(\mathbb{Q})$ donne aussi une estimation de la quantité Λ.

Théorème 14. *3. De l'inégalité $B(\mathbb{Q})$ il découle que pour tout $\varepsilon > 0$ et des entiers m et n premiers entre eux,*

$$\Lambda > \text{const} \cdot m^{-(2+b\varepsilon)},$$

où const > 0 *dépend seulement de ε.*

Démonstration. Posons $l = |m^a - n^b|$ et considérons plusieurs cas.

Cas 1. $m^a > n^b$ et $l > n^b$.

$$\Lambda = a \log m - b \log n = \log(1 + l/n^b) \geq \log 2.$$

Cas 2. $m^a < n^b$ et $l < n^b$. Posons $f = m^a/l$ et estimons les défauts :

(a) $\delta_0 \geq a - 1$;

(b) $\delta_\infty = \dfrac{\log l_1 + a \log m - \log l - 1}{a \log m} \geq 1 - \dfrac{\log l}{a \log m} - \dfrac{\text{const}}{a \log m}$;

(c) $\delta_1 \geq \dfrac{\log n^b - \log n}{a \log m}$;

(d) $\delta_2 \geq 0$.

Appliquons l'inégalité $B(\mathbb{Q})$ et obtenons

$$\log l \geq \log n^b - \log n - \log m - a\varepsilon \log m - \text{const}.$$

Par conséquent,

$$\frac{l}{n^b} \geq \frac{1}{\text{const} \cdot n \cdot m \cdot m^{a\varepsilon}} \geq \frac{1}{\text{const} \cdot m^{2+\varepsilon a}}. \tag{5.4}$$

Enfin,

$$\Lambda = \log(1 + \frac{l}{n^b}) \geq \frac{l}{2n^b}, \quad \text{car } l/n^b < 1.$$

En combinant cette estimation avec (5.4), nous obtenons la démonstration dans le cas 2.

Cas 3. $n^b > m^a$ et $l > m^a$.

$$\Lambda = b \log n - a \log m = \log(1 + l/m^a) \geq \log 2.$$

Cas 4. $n^b > m^a$ et $l < m^a$. Posons $f = n^b/l$ et, en appliquant l'inégalité $B(\mathbb{Q})$, obtenons

$$\log l \geq \log m^a - \log m - \log n - b\varepsilon \log n - \text{const}.$$

Par conséquent,

$$\frac{l}{m^a} \geq \frac{1}{\text{const} \cdot m^{2+\varepsilon b}}. \tag{5.5}$$

Enfin,

$$\Lambda = \log(1 + \frac{l}{m^a}) \geq \frac{1}{2}\frac{l}{m^a}, \quad \text{car } l/m^a < 1.$$

En combinant cette estimation avec (5.5), nous obtenons la démonstration du théorème 3 dans le cas 4. Le théorème est démontré.

5.4. Nombres premiers singuliers. Soit $f \in \mathbb{Q}$, $f \neq 0$ et $f \neq \pm 1$.

Définition. Un nombre premier p est dit singulier (pour f), si $v_p(f) = 0$ et $f^p \equiv f \pmod{p^2}$.

L'ensemble de tous les nombres premiers singuliers sera noté S. Posons

$$S_k = \{p \in S | v_p(f^p - f) = k\}.$$

Théorème 15. *4. De l'hypothèse A il découle que pour tout $\varepsilon > 0$ l'inégalité suivante est satisfaite :*

$$\sum_{p\in S}\log(\frac{1}{1-p^{-1}})+\sum_{p\in S_3}\log p+2\sum_{p\in S_4}\log p+3\sum_{p\in S_5}\log p+\dots\leqslant$$

$$\leqslant \log m_0+\log n_0+\varepsilon\log m+\text{const},$$

où $f=m/n$ avec $m>n>0$ et $(m,n)=1$; const *ne dépend que de ε.*

Corollaire 16. *De l'hypothèse A il découle que la densité de l'ensemble S dans l'ensemble de tous les nombres premiers est nulle, et que l'ensemble $S_{\geqslant 3}=S_3\cup S_4\cup\dots$ est fini.*

Démonstration (du théorème 4). Considérons le corps $K=\mathbb{Q}(\mu_N)$. Pour un nombre premier p introduisons les notations $N=dp^r$, où $(p,d)=1$; π, un certain diviseur premier de p dans le corps K.

Il y a deux alternatives :

(1) Le défaut $\delta_\pi(f,K)$ n'est pas défini. C'est le cas si $v_p(f)=0$ et d_p ne divise pas N, où d_p est l'ordre de f dans $\mathbb{F}_p^*$.

(2) Le défaut est défini, c'est-à-dire soit $v_p(f)=0$, soit $v_p(f)\neq 0$ et $d_p|N$. Dans ce cas posons

$$\delta_p(N)=\sum_{\pi|p}\delta_\pi(f,K).$$

Lemme 17. *1.*

(i) Si $v_p(f)\neq 0$, alors $\delta_p(N)=\delta_p+[1-1/\varphi(p^r)]\log p/\log m$.

(ii) Si $v_p(f)=0$ et $d_p|N$, alors $\delta_p(N)=(a_p-1)\dfrac{\log p}{\log m}+[1-1/\varphi(p^r)]\dfrac{\log p}{\log m}$, où $a_p=v_p(f^p-f)$.

Le lemme 1 se démontre par un calcul direct.

Lemme 18. *2. Si $N\geqslant 3$, alors*

$$\frac{\chi(K)}{N}=\sum_{p|N}\log(\frac{1}{1-p^{-1}})-\log N-\frac{1}{2}\gamma.$$

Le lemme 2 découle immédiatement du calcul du discriminant du corps cyclotomique (voir [13]).

Passons à la démonstration du théorème 4. Comme l'hypothèse A est invariante par rapport au remplacement de f par $(-f)$ ou $(1/f)$, on considère que $f=m/n$, où $m>n>0$. En appliquant l'hypothèse A à la paire (K,f), nous obtenons l'inégalité

$$\sum_{p\in P_1}[\delta_p\ +(1-1/\varphi(p^r))\frac{\log p}{\log m}]+\sum_{p\in P_2}[(a_p-1)+(1-1/\varphi(p^r))]\frac{\log p}{\log m}$$

$$+\frac{\log f}{\log m}\leq 2+\frac{\log N}{\log m}-\sum_{p|N}\frac{1}{p-1}\frac{\log p}{\log m}+\frac{R_1(f)}{\log m}. \tag{5.6}$$

Ici $P_1 = \{p | v_p(f) \neq 0\}$ et $P_2 = \{p | v_p(f) = 0 \text{ et } d_p | N\}$. Affaiblissons l'inégalité (5.6), en procédant aux remplacements suivants :

$$(1) \quad 1 - \frac{1}{\varphi(p^r)} \geqslant 0 \ ;$$

$$(2) \quad \sum_{p|N} \frac{\log p}{p-1} \geqslant 0 \ ;$$

$$(3) \quad R_1(f) \leqslant \varepsilon \log m + \text{const.}$$

Nous obtenons l'inégalité

$$\sum_{p \in P_2} \frac{(a_p - 1) \log p}{\log m} \leqslant \frac{\log m_0 + \log n_0 + \log N + \varepsilon \log m + \text{const}}{\log m}. \tag{5.7}$$

Soient $p_1 < p_2 < \ldots$, tous les nombres premiers de S, d_i, l'ordre de f dans $\mathbb{F}_{p_i}^*$. Posons $N = \text{ppcm}(d_1, \ldots, d_s)$. Alors $p_1, \ldots, p_s \in P_2$ et $N \leqslant d_1 \ldots d_s \leqslant (p_1 - 1) \ldots (p_s - 1)$. En substituant cette estimation pour N dans (5.7) et en ne laissant dans le membre de gauche que $p_1, \ldots, p_s$, nous obtenons l'inégalité suivante :

$$\sum_1^s [(a_{p_i} - 1) \log p_i - \log(p_i - 1)] \leqslant \log m_0 + \log n_0 + \varepsilon \log m + \text{const.}$$

Comme le membre de droite ne dépend pas de s, nous obtenons l'inégalité

$$\sum_{p \in S} \log(\frac{1}{1 - p^{-1}}) + \sum_{a_p \geqslant 3} (a_p - 2) \log p \leqslant \log m_0 + \log n_0 + \varepsilon \log m + \text{const.}$$

Le théorème 4 est démontré.

Conclusion

1. Bien sûr, les versions proposées pour $\mathbb{P}^1$, les applications f, etc., ne sont pas définitives. Par exemple, la relation $\deg f^*(Q) = \deg(f) \deg(Q)$ n'est vraie qu'approximativement, et pour éliminer ce défaut, il faudrait apparemment considérer f comme une application multivaluée (au moins aux points archimédiens).

2. On pourrait formuler une version raffinée de l'hypothèse principale, qui tiendrait compte de la proximité de f aux racines de l'unité aux points archimédiens. En particulier, cela suffirait pour démontrer l'inégalité de Szpiro sur un corps arbitraire, ainsi que pour estimer l'ordre d'approximation des logarithmes des nombres algébriques. Cette version n'est pas donnée ici, car il n'y a pas de certitude dans les définitions de base.

3. Il est possible que l'examen de modèles d'applications multivaluées dans le cas géométrique puisse clarifier certains détails. Si l'on considère la correspondance $X \xleftarrow{\varphi} Z \xrightarrow{\psi} Y$ comme une application multivaluée $\varphi \circ \psi^{-1} = f$, alors en essayant d'écrire la formule de Hurwitz pour f, il apparaît des termes qui s'interprètent naturellement comme des défauts et qui peuvent être négatifs. Cela

rappelle la situation décrite au n° 3.3.

4. Il est possible que l'examen de la situation suivante puisse clarifier certains détails de la formule de Hurwitz. Soit V une surface linéaire non triviale au-dessus de la courbe X, $V_0 = X \times \mathbb{P}^1$. Soit $\varphi : V \to V_0$ un isomorphisme birationnel préservant la fibre générique. Le morphisme $f : X \to \mathbb{P}^1$ donne la section suivante $s = \varphi^{-1}(\text{graphe } f)$. Ne peut-on pas reconstruire la formule de Hurwitz pour f, connaissant seulement s et la géométrie de V ? Dans le cas numérique, $f \in K$ peut être considéré comme le point $(1 : f) \in \mathbb{P}^1$, et la géométrie de $\mathbb{P}^1$ est représentée par la théorie d'Arakelov et Faltings (voir [14, 15]). Du calcul du fibré canonique du $\mathbb{P}^1$ d'Arakelov, il ressort que ce n'est pas une surface linéaire non triviale sur $\mathbb{Z}$.

5. Il est intéressant de comparer l'approche de ce travail avec celle de Vojta (voir [8]). Vojta travaille avec des points sur une variété arbitraire, mais son approche est basée sur une analogie avec la théorie de Nevanlinna et ne peut donc en principe pas donner des égalités. Du point de vue adopté dans ce travail, il faudrait considérer seulement des variétés "rigides" telles que $\mathbb{P}^1$, mais peut-être peut-on en dire beaucoup plus pour celles-ci.

Il serait intéressant à cet égard d'écrire l'analogue numérique des formules de Plücker pour les applications $f : X \to \mathbb{P}^n$.

6. Apparemment, la tâche la plus difficile est la définition de l'ordre de la "dérivée d'un élément d'un corps local par rapport à un paramètre local". Dans le cas fonctionnel, cet ordre peut être reconstruit à l'aide de la formule de Witt de la théorie des corps de classes (voir [1, 16]). Ne peut-on pas utiliser cette voie dans le cas numérique (voir [17, 18]) ? Peut-être faudrait-il considérer qu'au corps local correspond non pas un point, mais un ensemble entier d'états (à savoir le caractère quasi-quadratique du groupe multiplicatif), et chercher à définir $v(f')$ sous la forme $\sum_X \chi(f) w_X$. Pour clarifier les concepts de base, A. N. Parshin a proposé à l'auteur de prêter attention aux "formules explicites" (voir [19]). À ce propos, nous formulons deux questions :

1) Ne peut-on pas démontrer la formule de Hurwitz dans le cas fonctionnel en utilisant seulement les fonctions ζ et la théorie des corps de classes ?

2) Ne peut-on pas construire un objet remplaçant $\text{Gal}(F_N(\mathbb{P}^1))$, où $F_N(\mathbb{P}^1)$ est le "corps des fonctions rationnelles sur $\mathbb{P}^1/F_N$" ?

Références

[1] Chevalley C., *Groupes algébriques et corps de classes*, Mir, M., 1968.

[2] Szpiro L., *La conjecture de Mordell (d'après G. Faltings)*, Sem. Bourbaki, 36e an. 619 (1983/1984).

[3] Lang S., *Fondements de la géométrie diophantienne*, Mir, M., 1986.

[4] Stewart C. L., Tijdeman R., *On the Oesterlé–Masser conjecture*, Monats. Math. 102 (1986), 251–257.

[5] Masser D. W., *Note on a conjecture of Szpiro*, vol. 183, Astérisque, 1990, pp. 19–23.

[6] Mumford D., *Sur les équations définissant les variétés abéliennes*, Mathématiques 14, fasc. 1 (1970), 14, fasc. 2 (1970), 14, fasc. 5 (1970), 15, fasc. 2 (1971).

[7] Parshin A. N., *Sur l'application des revêtements ramifiés dans la théorie des équations diophantiennes*, Mat. Sb. 190, fasc. 2 (1989), 244–259.

[8] Vojta P., *Diophantine Approximations and Value Distribution Theory*, Lect. Notes Math. 1239 (1987).

[9] Tate J., *The Arithmetic of elliptic curves*, Invent. Math. (1974), 179–206.

[10] Deligne P., *Preuve de conjectures de Tate et de Shafarevich (d'après G. Faltings)*, Sem. Bourbaki, 36e an. 619 (1983/1984), 1–17.

[11] Feldman N. I., *Approximations des nombres algébriques*, Izd-vo MGU, M., 1981.

[12] Waldschmidt M., *A lower bound for linear forms in logarithms*, Acta Arithm. 37 (1980), 257–283.

[13] Lang S., *Les nombres algébriques*, Mir, M., 1966.

[14] Arakelov S. Yu., *Théorie des intersections des diviseurs sur une surface arithmétique*, Izv. AN SSSR. Ser. mat. 38, fasc. 6 (1974), 1179–1293.

[15] Faltings G., *Calculus on arithmetic surfaces*, Ann. Math. 119, no. 2 (1984), 387–424.

[16] Witt E., *Zyklische Körper und Algebren der Charakteristik p vom Grade p^n*, J. Crelle 176 (1936), 126–140.

[17] Shafarevich I. R., *Loi de réciprocité générale*, Mat. Sb. 26(68), fasc. 1 (1950), 113–146.

[18] Vostokov S. V., *Forme explicite de la loi de réciprocité*, Izv. AN SSSR. Ser. mat. 42, fasc. 6 (1978), 1288–1321.

[19] Weil A., *Sur les formules explicites de la théorie des nombres*, Izv. AN SSSR. Ser. mat. 36 (1972), 3–18.

Département de Saint-Pétersbourg
de l'Institut mathématique V. A. Steklov de l'Académie des sciences de Russie
191011, Saint-Pétersbourg, quai de la Fontanka, 27.

Reçu le 20 novembre 1991.