UNIVERSITÉ DE RENNES 1

2018

La conjecture ABC et quelques unes de ses conséquences

TER

Émeline Crouseilles et Alexandre Lardeur
Sous la direction de M. Bernard Le Stum

Résumé

In this paper, we are presenting the ABC conjecture in different forms, and a few of its consequences. We chose to talk mainly about the effective Mordell conjecture.
We can formulate the ABC conjecture as follows : for $\epsilon > 0$, there exists a constant C_ϵ such that for all a, b, $c \in \mathbb{Z}_{\neq 0}$ coprime, with $a + b = c$, then

$$\max(|a|, |b|, |c|) \leq C_\epsilon \mathrm{Rad}(abc)^{1+\epsilon}$$

where Rad(n) is the produce of its prime p. The ABC conjecture was first stated in 1985, by D. Masser and J. Oesterlé. One of the most important fact about it is that it implies the Fermat's last theorem, one of the biggest problem for three centuries in number theory.
We first show how the ABC conjecture implies the asymptotic Fermat's Last Theorem. Then, we develop tools in order to prove Mordell's Conjecture. Finally, we will talk about the Erdős-Woods conjecture, and the Wieferich primes, and the importance of the ABC conjecture is in these cases.

Table des matières

Chapitre 1

Introduction

1.1 Un premier exemple

Pour comprendre comment fonctionne cette conjecture, commençons par prendre trois éléments a, b, et c premiers entre eux. Prenons $a = 1024$, $b = 81$ et $c = 1105$. On a alors :

$$1024 + 81 = 1105.$$

On regarde la factorisation en nombres premiers.

$$2^{10} + 3^4 = 5 \times 13 \times 17.$$

Regardons le radical du produit de ces trois nombres, c'est-à-dire le produit de leurs facteurs premiers :

$$\mathrm{Rad}(abc) = 2 \times 3 \times 5 \times 13 \times 17 = 6630,$$

$$6630 > 1105.$$

Le radical du produit abc est plus grand que la somme c des deux premiers nombres. On a là un début de la formulation commune de la conjecture ABC. La conjecture ne s'arrête pas là car ce constat ne fonctionne pas tout le temps.

Contre-exemple : Prenons $a = 3$, $b = 125$ et donc $c = 128$.

$$3 + 125 = 128$$

$$3 + 5^3 = 2^7.$$

On a cette fois-ci $\mathrm{Rad}(abc) = 3 \times 5 \times 2 = 30 < 128$.

Ainsi, notre conjecture première ne fonctionne pas ici. *Que doit-on en penser ?* En faisant des tests, on verra clairement que le premier cas est bien plus fréquent que le second. De plus, si l'on porte le radical à une puissance supérieure à 1, on a un constat encore plus étrange : si pour $\mathrm{Rad}(abc)^k$ l'exposant k vaut 1, on obtiendra un nombre infini d'exceptions. Si, en revanche, k vaut une puissance supérieure *stricte* à 1, même d'extrêmement peu, alors il n'existerait qu'un nombre fini d'exceptions. On obtient finalement la conjecture suivante, donnée par D. Masser et J. Oesterlé en 1985 :

Conjecture ABC Soit $\epsilon > 0$. Il existe une constante C_ϵ positive telle que pour tout triplet d'entiers (a, b, c) premiers entre eux vérifiant $a + b = c$, on ait :

$$\max(|a|, |b|, |c|) \leq C_\epsilon \times \mathrm{Rad}(abc)^{1+\epsilon}.$$

1.2 Les différentes conjectures

De ces exemples, nous pouvons aboutir à plusieurs conjectures, qui n'ont pas toutes le même poids. Nous travaillons ici dans l'anneau des entiers $\mathbb{Z}$. Ce dernier étant factoriel, tout $n \in \mathbb{Z}$ a une unique décomposition :

$$n = (-1)^{e_0} p_1^{e_1} \dots p_k^{e_k}$$

où $p_1, \dots, p_k$ sont des nombres premiers distincts, $e_0 \in \{0, 1\}$ et où les $e_i \in \mathbb{N}$ pour $i = 1, \dots, k$.

Définition 1.1 (Radical)
On appelle radical de n, où $n = (-1)^{e_0} p_1^{e_1} \dots p_k^{e_k}$ la quantité suivante :

$$\mathrm{Rad}(n) := p_1 \dots p_k.$$

Exemple : $\mathrm{Rad}(1024) = \mathrm{Rad}(2^{10}) = 2$.

Définition 1.2 Pour $a, b, c \in \mathbb{Z}$ tel que $a + b = c$, on définit les quantités suivantes :

1. $h(a, b, c) := \max(\log|a|, \log|b|, \log|c|)$ (hauteur logarithmique),
2. $r(a, b, c) := \log \mathrm{Rad}(abc)$,
3. $L = \left\{ \dfrac{h(a,b,c)}{r(a,b,c)} : a, b, c \in \mathbb{Z},\ a + b = c\,;\ \mathrm{pgcd}(a, b, c) = 1 \right\}$.

On a alors une première conjecture :

Conjecture 1 (*ABC* Faible) $\sup L < \infty$.

En d'autres termes, il existe $C \in \mathbb{R}_+$ telle que $\forall\, a, b, c \in \mathbb{Z}, a+b = c; \mathrm{pgcd}(a, b, c) = 1$:

$$h(a, b, c) \leqslant C \times r(a, b, c).$$

Cette conjecture ne donne pas de grandes précisions sur la borne de L. Dans les exemples vus précédemment, on apprécierait de mettre 1 au lieu de ∞, mais l'exemple vu en première partie nous montre que cela ne fonctionne pas. W. Jastrzebowski et D. Spielman ont donné un nombre infini de ces exemples.

Lemme 1.1 $2^n | 3^{2^n} - 1$.

Démonstration. On procède par récurrence :

Pour $n = 0$, $2^n = 1$ divise $3^{2^0} - 1 = 2$.

Supposons que pour un certain $n \in \mathbb{N}$, $2^n | 3^{2^n} - 1$. Il existe donc $k \in \mathbb{Z}$ tel que

$$3^{2^n} - 1 = 2^n k.$$

On a alors :

$$\begin{aligned} 3^{2^{n+1}} - 1 &= (3^{2^n})^2 - 1 \\ &= (3^{2^n} - 1)(3^{2^n} + 1) \\ &= 2^n k((2^n k + 1) + 1) \\ &= 2^{n+1} k(2^{n-1} + 1) \\ &= 2^{n+1} k'. \end{aligned}$$

Donc $2^{n+1} | 3^{2^{n+1}} - 1$ d'où le résultat.

□

Proposition 1.2 Il existe une infinité de $a, b, c \in \mathbb{Z}$ avec $a + b = c$ et $\text{pgcd}(a, b, c) = 1$ qui vérifient $\dfrac{h(a,b,c)}{r(a,b,c)} > 1$.

Démonstration. On définit les suites suivantes :

$$a_n = 3^{2^n} \quad b_n = -1 \quad c_n = 3^{2^n} - 1.$$

Chaque triplet (a_n, b_n, c_n) vérifie $\begin{cases} a_n + b_n = c_n \\ \text{pgcd}(a_n, b_n, c_n) = 1. \end{cases}$

On a alors $h(a_n, b_n, c_n) = \log a_n = 2^n \log 3$, et :

$$\begin{aligned} r(a_n, b_n, c_n) = \log \text{Rad}(a_n b_n c_n) &\leq \log \text{Rad}(a_n) \text{Rad}(c_n) \\ &\leq \log \text{Rad}(a_n) + \log \text{Rad}(c_n) \\ &= \log 3 + \log \text{Rad}(c_n). \end{aligned}$$

Comme $c_n = 3^{2^n} - 1$, via le lemme précédent, $2^n | c_n$, donc il existe $k \in \mathbb{Z}$ tel que $c_n = 2^n k$, c'est-à-dire $k = \dfrac{c_n}{2^n}$. Ainsi :

$$\begin{aligned} \log \text{Rad}(c_n) = \log \text{Rad}(2^n k) &\leq \log \text{Rad}(2^n) \text{Rad}(k) \\ &= \log 2 + \log \text{Rad}(\frac{c_n}{2^n}) \\ &\leq \log 2 + \log \frac{c_n}{2^n}. \end{aligned}$$

On a finalement :

$$r(a_n, b_n, c_n) \leq \log 3 + \log 2 + \log \frac{c_n}{2^n} \leq \log 4 + \log 2 + \log \frac{c_n}{2^n} \leq \log c_n - (n-3) \log 2.$$

Et :

$$\frac{r(a_n, b_n, c_n)}{h(a_n, b_n, c_n)} \leq \frac{\log c_n - (n-3) \log 2}{2^n \log 3} \leq 1 - \frac{(n-3) \log 2}{2^n \log 3} < 1 \text{ si } n \geq 4.$$

□

Remarque : Concrètement, cela montre qu'on ne peut pas généraliser ce qu'on a vu dans le tout premier exemple ($c < \mathrm{Rad}(abc)$).

On a ensuite une seconde conjecture :

Conjecture 2 (ABC non-effective) $\limsup L = 1$.

Une forme dite effective est la suivante :

Conjecture 3 (ABC effective) Pour $\epsilon > 0$ il existe une constante calculable C_ϵ telle que pour tout $a, b, c \in \mathbb{Z}$ avec $\mathrm{pgcd}(a, b, c) = 1$ et $a + b = c$ on ait :

$$h(a, b, c) \leq (1 + \epsilon) r(a, b, c) + C_\epsilon.$$

Cette inégalité peut se réécrire sous la forme vue précédemment :

$$\max(|a|, |b|, |c|) \leq C_\epsilon \, \mathrm{Rad}(abc)^{1+\epsilon}.$$

Remarque : La constante C_ϵ n'est pas exactement la même dans chacune des formules données ci-dessus. Nous utiliserons en revanche cette même forme pour la constante dans la conjecture ABC dans le reste du papier par abus de notation.

On peut généraliser les trois conjectures sous la forme suivante :

$$h(a, b, c) \leq (\alpha + \epsilon) r(a, b, c) + C_\epsilon.$$

ABC faible nous donne alors que $\alpha < \infty$, ABC non-effective que $\alpha = 1$ et ABC effective indique que C_ϵ est calculable pour $\epsilon > 0$.

Une version plus précise a été donnée par Alan Baker en 2004 :

$$\max(|a|, |b|, |c|) \leq \frac{6}{5} \mathrm{Rad}(abc) \frac{(\log \mathrm{Rad}(abc))^\omega}{\omega!}.$$

où $\omega = \omega(abc)$ est le nombre de premiers distincts divisant a, b et c. Cela permet d'obtenir la formule suivante :

$$\max(|a|, |b|, |c|) < \mathrm{Rad}(abc)^{\frac{7}{4}}. \qquad (*_1)$$

Remarque : La dernière formule a été déduite par S. Laishram et T. N. Shorey dans [5].

Chapitre 2

Le théorème de Fermat et la conjecture ABC

La conjecture ABC a pour la première fois été énoncée lors d'une discussion entre Joseph Oesterlé, de l'université de Paris VI, et David Masser, de l'université de Bâle en Suisse, en 1985. Il est important de noter que cette conjecture n'a pas encore de démonstration reconnue. Cependant, en 2012, Shinichi Mochizuki a publié un article de 500 pages (environ) proposant une démonstration, utilisant des outils qu'il a lui-même créés. Cette dernière n'a pas encore été approuvée par la communauté scientifique.

Le constat le plus impressionnant à l'époque était que la conjecture pouvait démontrer le dernier théorème de Fermat, là où une véritable démonstration n'a été donnée qu'en 1994 par Andrew Wiles. Ce théorème avait été énoncé au XVIIème siècle par Pierre de Fermat. Avant 1994, il avait déjà été démontré qu'il n'existait pas de solutions pour de nombreuses valeurs de n, et que pour une démonstration complète du théorème il suffisait de le montrer pour n premier et pour $n = 4$.

2.1 Théorème de Fermat asymptotique

Le théorème de Fermat asymptotique est une version plus faible du dernier théorème de Fermat, dont voici l'énoncé.

Théorème 1 (Dernier théorème de Fermat)
Il n'existe pas de triplet (x, y, z) d'entiers positifs non nuls tel que $x^n + y^n = z^n$ si $n > 2$.

Il existe une infinité de solutions non triviales pour $n = 2$: ce sont les triplets Pythagoriciens.

Exemples

- $3^2 + 4^2 = 5^2$
- $5^2 + 12^2 = 13^2$

La conjecture ABC nous permet de démontrer la version asymptotique du dernier théorème de Fermat :

Théorème 2 La conjecture ABC implique qu'il existe $K_1 > 0$ tel que pour tout $n > K_1$, l'équation $x^n + y^n = z^n$ pour x, y, z entiers positifs non nuls n'a pas de solution.

Démonstration. Soient x, y, z trois entiers positifs tels que $xyz \neq 0$, et $x^n + y^n = z^n$. Quitte à diviser ces trois nombres par leur pgcd, on peut appliquer la conjecture ABC qui nous donne que

$$\max(x^n, y^n, z^n) \leq K_\epsilon \ \mathrm{Rad}(x^n y^n z^n)^{1+\epsilon}.$$

On a $\max(x^n, y^n, z^n) = z^n$. On obtient alors que

$$z^n \leq K_\epsilon \ \mathrm{Rad}(xyz)^{1+\epsilon}.$$

On sait que $\mathrm{Rad}(t) \leq t$ pour tout t. Ainsi, on a $\mathrm{Rad}(xyz) \leq xyz \leq z^3$. D'où

$$z^n \leq K_\epsilon \ z^{3+3\epsilon}$$

$$\Leftrightarrow \ln(z^n) \leq \ln(K_\epsilon \ z^{3+3\epsilon})$$

$$\Leftrightarrow n \ln(z) \leq \ln(K_\epsilon) + (3+3\epsilon)\ln(z).$$

Comme $z \geq 2$, on a :

$$n \ln(2) \leq \ln(K_\epsilon) + (3+3\epsilon)\ln(2)$$

$$\Leftrightarrow n \leq \frac{\ln(K_\epsilon)}{\ln(2)} + 3(1+\epsilon).$$

Si on choisit $\epsilon = 1$, on a finalement

$$n \leq 6 + \frac{\ln(K_1)}{\ln(2)}$$

et on obtient un majorant de n dépendant explicitement de K_1. □

En fait, en utilisant la conjecture $*_1$, on peut même montrer le dernier théorème de Fermat :

Démonstration. En reprenant les mêmes éléments que dans la preuve précédente et en posant $\epsilon = \frac{3}{4}$, on obtient l'inégalité suivante :

$$\begin{aligned} z^n &< \mathrm{Rad}(xyz)^{\frac{7}{4}} \\ z^n &< (xyz)^{\frac{7}{4}} \\ z^n &< z^{\frac{21}{4}} \\ n &< \tfrac{21}{4} < 6. \end{aligned}$$

Donc on obtient que $n < 6$; or il existe des preuves du théorème de Fermat pour $n = 3, 4, 5$ (voir [4]), ce qui achève la preuve.

□

2.2 Le théorème de Fermat généralisé

La conjecture ABC permet donc de démontrer le dernier théorème de Fermat, mais ne s'arrête pas là. Nous allons montrer ici qu'elle permet de démontrer le théorème de Fermat généralisé. On considère l'équation suivante :

$$Ax^r + By^s = Cz^t.$$

En prenant $A = B = C = 1$ et $r = s = t$ on obtient l'équation de Fermat. On a alors le théorème suivant :

Théorème 3 (Darmon et Granville)
Soient r, s et t trois entiers positifs vérifiant $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$, et soient A, B et C trois entiers fixés. Alors l'équation généralisée de Fermat n'a qu'un nombre fini de solutions entières telles que $\text{pgcd}(Ax, By) = 1$.

Démonstration. Une démonstration non fondée sur la conjecture existe (voir [3]). □

La conjecture ABC implique le théorème précédent. Pour cela, on commence par faire la remarque suivante :

Lemme 2.1 Pour trois entiers positifs non nuls r, s et t vérifiant

$$\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1, \qquad (*_2)$$

alors

$$\frac{1}{r} + \frac{1}{s} + \frac{1}{t} \leq 1 - \frac{1}{42}.$$

Démonstration. Quitte à faire un changement de variables, on peut supposer que $r \leq s \leq t$. On a forcément $r \geq 2$ sinon $(*_2)$ ne fonctionne pas.
Attaquons-nous cas par cas à l'inégalité.

$r = 2$ Alors $(*_2)$ peut se réécrire $\frac{1}{s} + \frac{1}{t} < \frac{1}{2}$ donc $s \geq 3$.

$s = 3$ Alors $\frac{1}{t} < \frac{1}{2} - \frac{1}{3}$ nous donne $t \geq 7$ et donc $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} \leq \frac{1}{2} + \frac{1}{3} + \frac{1}{7} = \frac{41}{42}$.

$s = 4$ Alors $\frac{1}{t} < \frac{1}{2} - \frac{1}{4}$ nous donne $t \geq 5$ et donc $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} \leq \frac{1}{2} + \frac{1}{4} + \frac{1}{5} = \frac{19}{20}$.

$s \geq 5$ Alors, par hypothèse $t \geq 5$. La somme sera encore plus petite que dans le cas précédent.

$r = 3$ On a donc $s, t \geq 3$ et $\frac{1}{s} + \frac{1}{t} < \frac{2}{3}$.

$s = 3$ Alors $\frac{1}{t} < \frac{1}{3}$ ce qui nous donne $t \geq 4$ et finalement $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} \leq \frac{1}{3} + \frac{1}{3} + \frac{1}{4} = \frac{11}{12}$.

$s \geq 4$ Comme $t \geq s$, $t \geq 4$. D'où $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} \leq \frac{1}{3} + \frac{1}{4} + \frac{1}{4} = \frac{5}{6}$.

$r \geq 4$ On a alors $s, t \geq 4$ et alors $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}$.

□

Proposition 2.2 Les conjectures 2 et 3 impliquent le théorème précédent.

Démonstration. Soient $A, B, C, x, y, z, r, s, t$ vérifiant les conditions du théorème. On va appliquer la conjecture ABC aux trois éléments suivants : $a = Ax^r$; $b = By^s$; $c = Cz^t$. La condition $(Ax, By) = 1$ nous assure que $\text{pgcd}(a, b, c) = 1$. Notre objectif est alors de borner la hauteur logarithmique du triplet de points, ce qui va nous donner (via les propriétés des hauteurs) un nombre fini de solutions. Majorons en premier lieu le radical :

$$\begin{aligned} \text{Rad}(abc) = \text{Rad}(Ax^r By^s Cz^t) &\leq \text{Rad}(ABC)\,\text{Rad}(x)\,\text{Rad}\,(y)\,\text{Rad}\,(z) \\ &\leq \text{Rad}\,(ABC) \times xyz \\ &\leq \text{Rad}\,(ABC) \times \left(\frac{a}{A}\right)^{\frac{1}{r}} \left(\frac{b}{B}\right)^{\frac{1}{s}} \left(\frac{c}{C}\right)^{\frac{1}{t}}. \end{aligned}$$

On utilise le logarithme :

$$\begin{aligned} r\,(a, b, c) &= \log \text{Rad}\,(abc) \\ &\leq \frac{1}{r}\log\left(\frac{a}{A}\right) + \frac{1}{s}\log\left(\frac{b}{B}\right) + \frac{1}{t}\log\left(\frac{c}{C}\right) + \log \text{Rad}\,(ABC) \\ &\leq \left(\frac{1}{r} + \frac{1}{s} + \frac{1}{t}\right) h\,(a, b, c) + \log \text{Rad}\,(ABC) \\ &\quad - \frac{\log|A|}{r} - \frac{\log|B|}{s} - \frac{\log|C|}{t}. \end{aligned}$$

Par le lemme précédent :

$$r\,(a, b, c) \leq \left(1 - \frac{1}{42}\right) \times h\,(a, b, c) + K_{A,B,C}.$$

avec $K_{A,B,C}$ constante calculable dépendante de A, B, C.
On utilise ensuite la conjecture ABC pour un $\epsilon > 0$:

$$h\,(a, b, c) \leq (1 + \epsilon)\, r\,(a, b, c) + C_\epsilon.$$

On remplace par ce que l'on a trouvé ci-haut et on obtient :

$$h\,(a, b, c) \leq (1 + \epsilon)\,[\left(1 - \frac{1}{42}\right) \times h\,(a, b, c) + K_{A,B,C}] + C_\epsilon$$

$$\left(1 - (1 + \epsilon)\left(1 - \frac{1}{42}\right)\right) h\,(a, b, c) \leq (1 + \epsilon)\, K_{A,B,C} + C_\epsilon.$$

La conjecture 3 nous donne alors des informations si $(1-(1+\epsilon)\left(1 - \frac{1}{42}\right) > 0$, soit lorsque $\epsilon < \frac{1}{41}$. On pourra alors calculer C_ϵ pour $\epsilon < \frac{1}{41}$ et $K_{A,B,C}$, ce qui nous donne une borne supérieure *connue* pour l'ensemble des solutions de l'équation de Fermat généralisée.
Si on suppose uniquement la conjecture 2, on obtient tout de même une borne pour $h(a, b, c)$ et comme il existe un nombre fini d'éléments vérifiant $h(a, b, c) \leq K_0$ pour un K_0 fixé, on a un nombre fini de solutions à l'équation demandée. □

Remarque : La preuve ici nous permet de prouver qu'il existe un nombre fini de solutions à l'équation de Fermat généralisée tout en permettant à r, s, t de **varier**. Le résultat est plus fort que le théorème démontré par Darmon et Granville.

Chapitre 3

La conjecture de Mordell

3.1 Énoncé

Conjecture 4 (conjecture de Mordell) Soit $\mathcal{C}$ une courbe algébrique définie sur $\mathbb{Q}$ de genre $g \geq 2$. Alors la courbe n'a qu'un ensemble fini de points à coordonnées rationnelles.

Par exemple, si on prend la courbe donnée par l'équation $y^2 = x^5 + x + 1$ de genre 2, la conjecture de Mordell nous dit donc que $x^5 + x + 1$ n'est le carré d'un nombre rationnel que pour un nombre fini de x rationnels.

La conjecture de Mordell, faite en 1922, est désormais connue sous le nom de Théorème de Faltings, dû à Gerd Faltings, mathématicien allemand qui a réussi en 1983 à la démontrer, et qui a obtenu la médaille Fields en 1986 en récompense de sa démonstration.

En 1991, Vojta donna une toute autre démonstration utilisant les techniques d'approximation diophantiennes. La démonstration que nous allons étudier ici provient d'un article publié par Machiel Van Frankenhuysen, qui utilise la conjecture ABC et les fonctions de Belyi (voir [9]). L'intérêt de cette démonstration (et de l'utilisation de la conjecture ABC) réside dans le fait que c'est uniquement avec elle qu'on peut obtenir une borne supérieure sur la hauteur des points, là où les autres démonstrations ne peuvent obtenir une borne *explicite* que sur le nombre de points dans $\mathcal{C}(\mathbb{Q})$. Nous allons donc développer l'ensemble des outils nécessaires à cette démonstration.

3.2 Définitions et outils

A) Valuations

Définition 3.1 (Valuation)
Une valuation de $\mathbb{Q}$ est une application

$$v : \mathbb{Q} \longrightarrow \mathbb{R} \cup \{-\infty\}$$

vérifiant :

- $v(x) = -\infty \iff x = 0$,

- $v(xy) = v(x) + v(y)$, $\forall x, y \in \mathbb{Q}^*$,
- $v(x+y) \leq K + \max\{v(x), v(y)\}$, $\forall x, y \in \mathbb{Q}$, K constante.

Remarque : La définition donnée ici de la valuation est particulière au papier, et ne reflète pas la définition générale des valuations. Nous reprenons seulement celle utilisée par Machiel Van Frankenhuysen ([9]).
Si p est premier, on note $\mathrm{ord}_p(x)$ la puissance du facteur p dans x. Comme x est rationnel, $\mathrm{ord}_p(x)$ peut être négatif.

Définition 3.2 (Valuation p-adique)
Soit p premier. On définit une valuation p-adique sur $\mathbb{Q}$ de la façon suivante : $v_p(x) = -\mathrm{ord}_p(x)\log p$. Pour l'infini on a $v_\infty(x) = \log|x|$.

Propriétés
- $v_p(x+y) \leq \max(v_p(x), v_p(y))$ (v_p est non-archimédienne),
- $v_\infty(x+y) \leq \log 2 + \max(v_\infty(x), v_\infty(y))$ (v_∞ est archimédienne).

Remarque : La valuation triviale est définie par :

- $v(0) = -\infty$
- $v(x) = 0$ pour $x \neq 0$.

La valuation triviale et les valuations p-adique (ainsi que v_∞) représentent l'ensemble des valuations de $\mathbb{Q}$. Cela nous donne la formule suivante :

Proposition 3.1 (Formule de la somme.)

Soit $x \in \mathbb{Q}^*$. Alors :

$$\sum_v v(x) = 0. \qquad (*_3)$$

Démonstration. Soit $x \in \mathbb{Q}^*$. On peut écrire :

$$|x| = \prod_p p^{\mathrm{ord}_p(x)},$$

où les p sont premiers et presque tous nuls. D'où :

$$\log|x| = \sum_p \mathrm{ord}_p(x)\log p = v_\infty(x).$$

Finalement,

$$\begin{aligned}
\sum_v v(x) &= \sum_p v_p(x) + v_\infty(x) \\
&= \sum_p -\mathrm{ord}_p(x)\log p + \log|x| \\
&= -\sum_p \mathrm{ord}_p(x)\log p + \sum_p \mathrm{ord}_p(x)\log p \\
&= 0.
\end{aligned}$$

□

B) La conjecture ABC dans l'espace projectif $\mathbb{P}^2$

Pour démontrer la conjecture, nous allons avoir besoin d'utiliser la conjecture ABC dans le plan projectif sur $\mathbb{Q}$, que l'on note $\mathbb{P}^2(\mathbb{Q})$. On rappelle que $\mathbb{P}^2(\mathbb{Q})$ est l'ensemble des points $(x : y : z)$, avec $x, y, z \in \mathbb{Q}$, non tous nuls, tels que pour $\lambda \in \mathbb{Q}^*$, les points $(x : y : z)$ et $(\lambda x : \lambda y : \lambda z)$ désignent le même point dans $\mathbb{P}^2(\mathbb{Q})$. Des équations homogènes donnent des sous-ensembles dans $\mathbb{P}^2$. Nous allons ici considérer en particulier le sous-ensemble donné par l'équation $x + y = z$, qui se trouve être une *droite* dans $\mathbb{P}^2(\mathbb{Q})$.

Le point $(0 : 0 : 0)$ n'est pas un point de $\mathbb{P}^2(\mathbb{Q})$. On dit que c'est un point *indéterminé*.

Définition 3.3 (Hauteur)
La hauteur d'un point $P = (a : b : c) \in \mathbb{P}^2(\mathbb{Q})$ est définie par :

$$h(P) = \sum_v \max\{v(a), v(b), v(c)\}$$

où v parcourt l'ensemble des valuations p-adiques de $\mathbb{Q}$ (exceptée la valuation *triviale*).

Définition 3.4 (Radical)
Si $a, b, c \in \mathbb{Q}$ sont non nuls, on définit le radical de P par :

$$r(P) = r(a : b : c) = \sum_{p : \#\{v_p(a), v_p(b), v_p(c)\} \geq 2} \log p.$$

Remarque : Ces définitions ne dépendent pas du choix des coordonnées de P. En effet, pour le radical, on remarque, en prenant comme point $(\lambda a : \lambda b : \lambda c)$, que : $v_p(\lambda x) = v_p(\lambda) + v_p(x)$, et ainsi : $\{v_p(\lambda a), v_p(\lambda b), v_p(\lambda c)\} = \{v_p(\lambda) + v_p(a), v_p(\lambda) + v_p(b), v_p(\lambda) + v_p(c)\}$, et donc le cardinal de cet ensemble ne diffère pas de celui de $\{v_p(a), v_p(b), v_p(c)\}$. Pour la hauteur, on utilise la formule de la somme $(*_3)$.

$$\begin{aligned} h(\lambda a : \lambda b : \lambda c) &= \sum_v \max\{v(\lambda a), v(\lambda b), v(\lambda c)\} \\ &= \sum_v \max\{v_p(\lambda) + v_p(a), v_p(\lambda) + v_p(b), v_p(\lambda) + v_p(c)\} \\ &= \underbrace{\sum_v v(\lambda)}_{=0} + \sum_v \max\{v(a), v(b), v(c)\}. \end{aligned}$$

En prenant des triplets premiers entre eux, avec $a + b = c$, on remarque que ces définitions coïncident avec celles de la définition 1.2.

Définition 3.5 (Terme d'erreur)
On définit le terme d'erreur de P la quantité :

$$e(P) = e(a : b : c) = \max\{h(P) - r(P), 0\}.$$

On obtient la reformulation suivante pour la conjecture ABC :

Conjecture 5 (ABC dans $\mathbb{P}^2$) Pour tout $\varepsilon > 0$ il existe une constante $K(\varepsilon)$ tel que

$$e(P) \leq \varepsilon h(P) + K(\varepsilon)$$

pour tout point $P = (a : b : c) \in \mathbb{P}^2(\mathbb{Q})$ sur la droite $a + b = c$ avec $abc \neq 0$.

De nombreuses conjectures ont été faites depuis la première version de J. Oesterlé et D. Masser, qui permettent d'expliciter et d'obtenir des valeurs numériques de la constante $K(\varepsilon)$ (un exemple est donné plus haut $*_1$).

Admettons que dans la conjecture 5, $K(\varepsilon)$ est donnée explicitement comme fonction de ε. On détermine alors, pour chaque valeur de h, le minimum $\psi(h)$ de $\varepsilon h + K(\varepsilon)$,

$$\psi(h) = \min_{\varepsilon > 0} \varepsilon h + K(\varepsilon)$$

Ainsi, on peut réécrire 5 comme :

$$e(P) \leq \psi(h(P)) \qquad (*_4)$$

pour une certaine fonction $\psi(h) = o(h)$.

C) La théorie des hauteurs

Pour démontrer la conjecture de Mordell nous avons besoin de définir certaines fonctions hauteurs, qui ici ne seront définies que sur $\mathbb{Q}$. Tout d'abord, une fonction hauteur H sur une variété est une fonction qui à un point P associe la valeur $H(P)$ qui mesure la *complexité arithmétique* du point. Par exemple, si on prend $\frac{1}{2}$ et $\frac{10000}{20001}$, ces deux nombres sont proches l'un de l'autre, mais intuitivement le second est plus compliqué *arithmétiquement* que le premier.

On rappelle la définition de hauteur vue dans la partie précédente, qu'on peut ici généraliser sur $\mathbb{P}^n(\mathbb{Q})$.

Définition 3.6 (Hauteur logarithmique)
Pour un point $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n(\mathbb{Q})$, on définit sa hauteur logarithmique (que l'on nommera dans la suite juste *hauteur*) par :

$$h(x) = \sum_v \max\{v(x_0) : \ldots : v(x_n)\}.$$

Propriété importante : Pour tout $C > 0$, l'ensemble $\{x \in \mathbb{P}^n(\mathbb{Q}) : h(x) \leq C\}$ est fini.

Une propriété qui va nous être tout aussi utile est la suivante : pour un point x, un morphisme de degré d multiplie sa hauteur par d, c'est-à-dire :

Proposition 3.2 $f : \mathbb{P}^N(\mathbb{Q}) \to \mathbb{P}^M(\mathbb{Q})$ une application de degré d. Il existe une constante C tel que :

$$dh(x) - C \leq h(f(x)) \leq dh(x) + C \quad \forall x \in \mathbb{P}^N(\mathbb{Q}).$$

Démonstration. La démonstration est en deux temps, avec plus de facilité pour la majoration. Nous renvoyons à [7] et [2] pour plus de détails. □

Remarque : Les constantes dépendent de l'application. Ainsi, si l'on s'intéresse à l'application $P : (a : b) \mapsto (a : b : a + b)$ on obtient :

$$h(x) \leq h(P(x)) \leq h(x) + \log 2. \qquad (*_5)$$

Pour finir, nous allons avoir besoin de définir une hauteur sur une courbe algébrique non singulière $\mathcal{C}$. On choisit alors une application $f : \mathcal{C} \to \mathbb{P}^1$. Si f est de degré d, on définit la hauteur $h(x) = h_f(x)$, pour $x \in \mathcal{C}(\mathbb{Q})$ de la façon suivante :

$$h(x) = h_f(x) = \frac{1}{d} h(f(x)).$$

Si de plus, on prend un autre morphisme $g : \mathcal{C} \to \mathbb{P}^1$, il existe une constante K telle que

$$|h_f(x) - h_g(x)| \leq K\sqrt{h_f(x)}. \qquad (*_6)$$

D) Ramification et formule d'Hurwitz

Soit $f : \mathcal{C} \to \mathcal{C}'$ une application entre deux courbes algébriques non singulières. En travaillant avec des valeurs complexes, on obtient une application entre surfaces de Riemann. Pour un point $y \in \mathcal{C}'(\mathbb{C})$, $f^{-1}\{y\}$ contient presque toujours le même nombre d'antécédents, que l'on va noter d. Ce nombre d est appelé *degré* de f, noté $d = \deg f$. Seulement, pour un nombre fini de points y, l'ensemble des antécédents peut contenir moins de d points. Ainsi, quand $\#f^{-1}\{y\} < \deg f$, on dit que f est *ramifiée sur* y.

Pour un point $x \in \mathcal{C}(\mathbb{C})$, en général f envoie un (petit) voisinage de x injectivement sur un petit voisinage de $f(x)$ dans $\mathcal{C}'(\mathbb{C})$. Pour un nombre fini de points x, l'application n'est injective pour aucun voisinage de x. Pour ces points, on dit que f est *ramifiée en* x. Dans ce cas, il existe un nombre $e \geq 2$ et un petit voisinage U de x dans $\mathcal{C}(\mathbb{C})$ tel que l'image de $U - \{x\}$ par f a e antécédents. Ce nombre e est appelé *multiplicité* de f en x, noté $e_x(f)$. Ainsi, f n'est pas ramifié en x si et seulement si $e_x(f) = 1$.

Nous avons que f est *ramifiée sur* y si et seulement si f est *ramifiée en* un certain point x, avec $f(x) = y$. Soit $g : \mathcal{C}' \to \mathcal{C}''$ une autre application. Alors $\deg(g \circ f) = \deg f \times \deg g$, et $g \circ f$ est ramifiée exactement en tout point où f l'est aussi, et en tout point $x \in \mathcal{C}(\mathbb{C})$ tel que g est ramifiée en $f(x)$. De même, $g \circ f$ est ramifiée sur chaque point où g est ramifiée et sur chaque point $z \in \mathcal{C}''$ tel que f est ramifiée sur des points dans $g^{-1}\{z\}$.
Lorsque l'on compte les points de $f^{-1}\{y\}$ avec leur multiplicité, on aura toujours le degré de f,

$$\text{pour tout } y \in \mathcal{C}'(\mathbb{C}) : \sum_{x\,:\, f(x)=y} e_x(f) = \deg f. \qquad (*_7)$$

Nous allons aussi avoir besoin de la formule d'Hurwitz, qui relie la ramification de f avec le genre de $\mathcal{C}$ et de $\mathcal{C}'$:

$$2g(\mathcal{C}) - 2 = (2g(\mathcal{C}') - 2) \times \deg f + \sum_{x \in \mathcal{C}(\mathbb{C})} (e_x(f) - 1). \qquad (*_8)$$

Remarque : La somme à droite est finie, car il n'existe qu'un nombre fini de x tels que $e_x(f) > 1$.
En appliquant la formule à l'application $z \mapsto z^2$ de $\mathbb{P}^1$ vers $\mathbb{P}^1$, on obtient que le genre de $\mathbb{P}^1$ est 0. En effet, l'application utilisée est de multiplicité 2 en 0, donc ramifiée en 0, et de même en l'infini, ce qui donne :

$$\begin{aligned} 2g(\mathbb{P}^1) - 2 &= (2g(\mathbb{P}^1) - 2) \times 2 + \sum_{f(x)=0,\infty} (e_x(f) - 1) \\ 2g(\mathbb{P}^1) - 2 &= 4g(\mathbb{P}^1) - 4 + 2 \\ g(\mathbb{P}^1) &= 0. \end{aligned}$$

Finalement, si $f : \mathcal{C} \to \mathbb{P}^1$ est une fonction uniquement ramifiée en 0, 1 ou ∞, la formule se réécrit de la façon suivante :

$$\begin{aligned} 2g(\mathcal{C}) - 2 &= -2 \deg f + \sum_{f(x)=0,1,\infty} (e_x(f) - 1) \\ &= \deg f - \#f^{-1}\{0, 1, \infty\} \end{aligned} \qquad (*_9)$$

d'après $(*_7)$ et $(*_8)$.

E) Théorie des diviseurs

Définition 3.7 (Diviseur)
Soit $\mathcal{C}(\mathbb{C})$ une surface de Riemann. On appelle diviseur une somme finie

$$D = e_1x_1 + e_2x_2 + ... + e_kx_k$$

avec $x_1, ..., x_k \in \mathcal{C}(\mathbb{C})$ et $e_1, ..., e_k \in \mathbb{Z}$. On dit que $e_i = \mathrm{ord}_{x_i}(D)$ est l'*ordre* de D en x_i. Donc, on a :

$$D = \sum_{x \in \mathcal{C}(\mathbb{C})} \mathrm{ord}_x(D)(x).$$

Un diviseur D est positif, $D \geq 0$, si $\mathrm{ord}_x(D) \geq 0$ pour tout $x \in \mathcal{C}(\mathbb{C})$. On écrit $D \leq D'$ pour $D' - D \geq 0$. De plus, le *degré* de D est $\deg D = e_1 + ... + e_k$.
Enfin, on appelle *support* de D l'ensemble $\sup D = \{x \in \mathcal{C}(\mathbb{C}) : \mathrm{ord}_x(D) \neq 0\}$.

Définition 3.8 (a-diviseur)
Soit $f : \mathcal{C} \to \mathbb{P}^1$ et soit $a \in \mathbb{P}^1(\mathbb{C})$. Alors le a-diviseur de f est donné par

$$f^*(a) = \sum_{x \in f^{-1}(\{a\})} e_x(f)(x).$$

De plus, $\deg f^*(a) = \deg f$.

Définition 3.9 (Diviseur défini sur $\mathbb{Q}$, diviseur irréductible)
Soit $\mathcal{C}$ une courbe définie sur $\mathbb{Q}$. Tout plongement $\sigma : \bar{\mathbb{Q}} \to \mathbb{C}$ induit un plongement de $\mathcal{C}(\bar{\mathbb{Q}})$ dans $\mathcal{C}(\mathbb{C})$. Alors un diviseur positif D est défini sur $\mathbb{Q}$ si l'image $\sigma(D)$ ne dépend pas de σ.
De plus, un diviseur positif D défini sur $\mathbb{Q}$ est dit irréductible si on ne peut pas l'écrire comme somme de diviseurs positifs définis sur $\mathbb{Q}$.

Remarque : Si D est un diviseur positif, les applications $f : \mathcal{C} \to \mathbb{P}^1$ telles que $f^*(\infty) \leq D$ forment un espace vectoriel ; de plus, si D est défini sur $\mathbb{Q}$, en ne considérant que les f définies sur $\mathbb{Q}$, elles forment un $\mathbb{Q}$-espace vectoriel.
On note la dimension de cet espace par $l(D)$. Le théorème de Riemann-Roch nous donne que :

$$l(D) = \deg D + 1 - g,$$

si $\deg D \geq 2g - 1$ où g est le genre de $\mathcal{C}$.

Le lemme suivant nous sera très utile pour la démonstration de la conjecture de Mordell :

Lemme 3.3 Soit D un diviseur positif de $\mathcal{C}$ de genre g. Si $\deg D \geq 2g$, alors il existe une application $d : \mathcal{C} \to \mathbb{P}^1$ telle que $D = d^*(0)$.

Démonstration. Pour le cas $D = 0$ et $g = 0$, $D = 0$ est le 0-diviseur d'une application constante non nulle.
Soit $D > 0$ de degré $\geq 2g$. On écrit $D = \sum_{i=1}^{r} e'_i x_i$. Soit $x_j \in \sup(D)$ pour un certain $j \in \{1, \ldots, r\}$. On a alors :

$$\deg(D - (x_j)) = \deg D - 1 \geq 2g - 1.$$

Nous avons vu ci-dessus que pour un diviseur G $l(G) = \deg G + 1 - g$, c'est-à-dire $\deg G = l(G) - 1 + g$. On obtient finalement :

$$l(D - (x_j)) = l(D) - 1.$$

Comme $l(D - (x_j))$ est la dimension de l'espace vectoriel engendré par les applications f telles que $f^*(\infty) \leq D - (x_j)$, on voit que la dimension de $\{f : f^*(\infty) \leq D - (x_j)\}$ est plus petite que la dimension de $\{f : f^*(\infty) \leq D\}$; donc il existe une fonction f telle que $f^*(\infty) \leq D$ mais pas $f^*(\infty) \leq D - (x_j)$. On peut écrire $f^*(\infty) = \sum_{i=1}^{r} e_i x_i$ et donc $D - (x_j) = \sum_{i=1}^{r} (e'_i - \delta_{i,j}) x_i$, pour tout x_i.
D'une part, on a $f^*(\infty) \leq D$ donc $e_i \leq e'_i$.
D'autre part, $f^*(\infty) \leq D - (x_j)$, donc on obtient pour x_j que $e_j > e'_j - \delta_{j,j} = e'_j - 1$; autrement dit, $e_j = e'_j$.
Donc f a un pôle en x_j, d'ordre la multiplicité de x_j, car $e_j = e'_j$.
Pour chaque $x_j \in \sup(D)$, on peut trouver une fonction f_{x_j} qui a un pôle d'ordre $\mathrm{ord}_{x_j}(D)$ en x_j, et qui peut avoir d'autres pôles d'ordre au plus celui de D, mais pas plus. Ainsi, il existe une combinaison linéaire de ces fonctions, $f = \sum_{x \in \sup(D)} c_x f_{x,}$, avec $c_x \in \mathbb{Q}$, qui aura D comme diviseur.
Donc, en prenant $d = \frac{1}{f}$, on a bien que $D = d^*(0)$. □

F) Le théorème de Belyi

Théorème 4 Soit $\mathcal{C}$ une courbe algébrique définie sur $\mathbb{Q}$, et soit Σ un sous-ensemble de points algébriques de $\mathcal{C}$. Il existe une application $f : \mathcal{C} \to \mathbb{P}^1$, définie sur $\mathbb{Q}$ associée à Σ telle que f soit uniquement ramifiée sur 0, 1 et ∞, et $f(\Sigma) \subseteq \{0, 1, \infty\}$.

Démonstration. On procède par étapes.

Étape 1 : *On peut supposer que* $\mathcal{C} = \mathbb{P}^1$

Soit $g : \mathcal{C} \to \mathbb{P}^1$ une autre application définie sur $\mathbb{Q}$. On considère le sous-ensemble de $\mathbb{P}^1$ suivant :

$$\Sigma' = g(\Sigma) \cup \{x \in \mathbb{P}^1 : g \text{ est ramifiée sur } x\}.$$

S'il existe $h : \mathbb{P}^1 \to \mathbb{P}^1$ associée à Σ' et à $\mathbb{P}^1$ qui vérifie le théorème, on prend alors $f = h \circ g$. En effet, si $h(\Sigma') \subseteq \{0, 1, \infty\}$, pour $x \in \Sigma$,

$$f(x) = h \circ g(x) = h(\underbrace{g(x)}_{\in \Sigma'}) \subseteq \{0, 1, \infty\},$$

et f n'est bien ramifiée qu'en 0, 1 et ∞. Nous n'allons donc plus travailler qu'avec $\mathcal{C} = \mathbb{P}^1$, et $\Sigma \subset \mathbb{P}^1$ sous-ensemble de points algébriques.

Étape 2 : *On peut supposer que $\Sigma \subseteq \mathcal{C}(\mathbb{Q})$ et 0, 1, $\infty \in \Sigma$.*
Soit d le degré maximal sur $\mathbb{Q}$ des éléments de Σ, notons p le nombre d'éléments de Σ de degré d, et prenons $\alpha \in \Sigma$ de degré d. α est racine d'un polynôme $m(X)$, de degré d, à coefficients rationnels. On obtient l'application $m : \mathbb{P}^1 \to \mathbb{P}^1$,

$$m : (x_0 : x_1) \mapsto ({x_1}^d m(\frac{x_0}{x_1}) : {x_1}^d),$$

Cette application est ramifiée en ∞, et en tout point critique x, c'est à dire tel que $m'(x) = 0$. On considère maintenant le sous-ensemble suivant :

$$\Sigma' = m(\Sigma) \cup \{\infty\} \cup m(S)$$

où S est l'ensemble des éléments x tel que $m'(x) = 0$. $m(S)$ ne contient donc que des éléments de degré $\leq d-1$. Comme $m(\alpha) = 0$, et que pour tout $\gamma \in \Sigma$, le degré de $m(\gamma)$ est au plus celui de γ, Σ' contient au plus $p-1$ éléments de degré d.
En répétant cette étape, Σ ne contiendra finalement plus que des points rationnels. Nous pouvons enfin supposer que $\{0, 1, \infty\} \subseteq \Sigma$.

Étape 3 : *Réduction du nombre d'éléments de Σ.*
Supposons que Σ contienne 0, 1 et ∞, et un quatrième point $\alpha \in \mathbb{Q}$ différent des trois précédents, qu'on écrit $\alpha = a/c$, avec $a, c \neq 0$ et $a \neq c$. On considère maintenant la fonction

$$\varphi(x) = \lambda x^a (1-x)^{c-a}.$$

Cette application est ramifiée en 0, 1 et ∞, et en tout point x tel que $\varphi'(x) = 0$. De plus, $\varphi(x) = 0$ ou ∞ seulement pour 0, 1 ou ∞. Ainsi, si $x \neq 0$, 1, ∞, on a $\varphi'(x) = 0$ si et seulement si $\varphi'(x)/\varphi(x) = 0$. Cela nous donne :

$$\frac{\varphi'(x)}{\varphi(x)} = \frac{a}{x} - \frac{c-a}{1-x}$$

et on obtient en calculant que $\varphi'(x) = 0$ pour $x = a/c$. On choisit ensuite λ pour obtenir $\varphi(a/c) = 1$. Cela nous permet d'obtenir que φ est uniquement ramifiée en 0, 1 et ∞, et comme $\varphi\{0, 1, \infty\} = \{0, \infty\}$, $\varphi(\Sigma)$ contient moins d'éléments que Σ. En répétant cette étape, Σ ne contiendra finalement que 0, 1 et ∞.

□

G) Premier de bonne réduction

Définition 3.10 PREMIERS DE BONNE RÉDUCTION.
Soit $\mathcal{C}$ une courbe définie sur $\mathbb{Q}$ par l'ensemble des $(x_0 : ... : x_n) \in \mathbb{P}^n$ satisfaisant les équations :

$$\begin{cases} p_1(x_0, ..., x_n) &= 0 \\ \quad\vdots & \\ p_k(x_0, ..., x_n) &= 0 \end{cases}$$

où les p_i sont des polynômes homogènes, et soit $f : \mathcal{C} \to \mathbb{P}^m$ donnée par $m+1$ polynômes homogènes de même degré, définie sur $\mathbb{Q}$ par :

$$f : (x_0 : ... : x_n) \mapsto (f_0(x_0, ..., x_n) : ... : f_m(x_0, ..., x_n)).$$

On multiplie respectivement ces équations par un entier bien choisi de sorte que tous les coefficients soient entiers.
Soit p un nombre premier. On réduit chacun de ces coefficients modulo p, et on réduit aussi modulo p les variables utilisées. Un nombre algébrique α devient 0 si $v_p(\alpha) < 0$ et ∞ si $v_p(\alpha) > 0$. On note par une barre la réduction modulo p. Mais on peut obtenir des cas où la réduction modulo p devient problématique :

- Si l'équation devient "$0 = 0$",
- Si le degré de l'application f est diminué,
- Si l'application f devient indéterminée en certains points, c'est-à-dire si elle associe à un point le point $(0 : 0)$ (voir page 14),
- Si, pour un diviseur D de $\mathcal{C}$, modulo p, certains points de D coïncident ou deviennent indéterminés,
- Si, pour deux points distincts a et $b \in \mathbb{P}^1(\mathbb{Q})$, tel que f n'est pas ramifiée sur a, a ou b deviennent indéterminés, ou coïncident.

On enlève l'ensemble de ces p, dits de *mauvaise réduction*, en notant que cet ensemble est *fini* lorsqu'on fixe le diviseur.

On enlève aussi les p de mauvaise réduction (définis par les cas ci-dessus) pour les diviseurs $f^*(a)$ et $f^*(b)$.

Propriétés (PREMIERS DE BONNE RÉDUCTION.)
- $\bar{f}$ n'est pas constante.
- $\deg \bar{f} = \deg \bar{f}^*(\bar{a}) = \deg f$, pour $a \in \mathbb{P}^1(\mathbb{Q})$.

3.3 Démonstration de la conjecture de Mordell

Le principe de la démonstration est le suivant :

1. On construit une fonction de Belyi $f : \mathcal{C} \to \mathbb{P}^1$ avec certaines particularités.

2. On obtient avec la conjecture ABC que soit $x \in \mathcal{C}(\mathbb{Q})$ est envoyé par f sur 0, 1 ou ∞, soit la hauteur de $f(x)$ est bornée par une constante explicite.

Démonstration. Soit $f : \mathcal{C} \to \mathbb{P}^1$ une fonction de Belyi associée à la courbe $\mathcal{C}$, avec $\Sigma = \emptyset$. Alors f est bien définie sur $\mathbb{Q}$, et en particulier, on a $f(x) \in \mathbb{P}^1(\mathbb{Q})$ si $x \in \mathcal{C}(\mathbb{Q})$.
Soient A, B et C les diviseurs respectifs de f pour 0, 1 et ∞, autrement dit : $A = f^*(0)$, $B = f^*(1)$ et $C = f^*(\infty)$. Ces diviseurs ont une décomposition en diviseurs irréductibles :

$$\begin{aligned} A &= e_1 M_1 + \cdots + e_i M_i, \\ B &= e_{i+1} M_{i+1} + \cdots + e_j M_j, \\ C &= e_{j+1} M_{j+1} + \cdots + e_k M_k. \end{aligned}$$

On note d_ν le degré de M_ν et d le degré de f. Ll'ensemble des antécédents de chacun des éléments de $\{0, 1, \infty\}$ est égal à la somme des degrés de ses diviseurs (irréductibles),

autrement dit : $\#f^{-1}\{0\} = \sum_{\nu=1}^{i} d_\nu$, $\#f^{-1}\{1\} = \sum_{\nu=i+1}^{j} d_\nu$ et $\#f^{-1}\{\infty\} = \sum_{\nu=j+1}^{k} d_\nu$. La fonction f étant de Belyi, elle n'est ramifiée que sur $\{0, 1, \infty\}$ et en utilisant la formule d'Hurwitz, on a :

$$\#f^{-1}\{0, 1, \infty\} = \sum_{\nu=1}^{k} d_\nu = d + 2 - 2g < d.$$

Prenons maintenant un N assez grand tel que pour chaque ν, NM_ν soit donné comme le diviseur d'une fonction m_ν pour 0 :

$$NM_\nu = m_\nu^*(0).$$

Si on utilise le lemme 3.3, on peut prendre $N = 2g$.
Soit $x \in \mathcal{C}(\mathbb{Q})$ un point à coordonnées rationnelles tel que $f(x) \neq 0,\ 1,\ \infty$. Nous allons appliquer la conjecture ABC au point :

$$P = (f(x) : 1 - f(x) : 1)$$

et allons en déduire que la hauteur de x est bornée. Par $(*_5)$, on a $h(P) \geq h(f(x))$. Pour f, comme vue dans la partie sur la théorie des hauteurs $h(x) := h_f(x)$ et on obtient

$$h(P) \geq dh(x). \qquad (*_{10})$$

Cherchons maintenant une approximation du radical. Prenons p un nombre premier de bonne réduction pour $\mathcal{C}$, f, chaque m_ν et chaque M_ν. Le premier p permet d'obtenir $\log p$ dans le radical s'il satisfait la condition : $\#\{v_p(f(x)), v_p(1-f(x)), v_p(1)\} \geq 2$. Le premier p satisfait cette condition si $v_p(f(x)) > 0$ ou bien si $v_p(f(x)) < 0$ ou si $v_p(f(x)) = 0$, auquel cas il faut que $v_p(1 - f(x)) \neq 0$. Comme $v_p(1) = 0$ pour tout p, alors

$$\begin{aligned} v_p(1 - f(x)) &\leq \max[v_p(1), v_p(f(x))] \\ &\leq 0 \end{aligned}$$

donc il faut forcément que $v_p(1 - f(x)) < 0$ dans ce dernier cas.
En résumé, le premier p permet d'obtenir $\log p$ dans le radical si et seulement si $v_p(f(x)) > 0$, $v_p(f(x)) < 0$ ou $v_p(1 - f(x)) < 0$. Cela signifie que $\bar{f}(\bar{x}) = \bar{\infty}$, $\bar{0}$ ou $\bar{1}$. En effet, par exemple, si $v_p(f(x)) > 0$, par définition de la valuation p-adique, on a

$$v_p(f(x)) = -\operatorname{ord}_p(f(x)) \log p.$$

On obtient $\operatorname{ord}_p(f(x)) < 0$ si $v_p(f(x)) > 0$, ce qui nous donne modulo p que $\bar{f}(\bar{x}) = \bar{\infty}$. Le raisonnement est similaire dans le deuxième et le dernier cas.
Si $\bar{f}(\bar{x}) = \bar{\infty}$, $\bar{0}$ ou $\bar{1}$, alors $\bar{x}$ est dans le support d'un des diviseurs $\bar{A}$, $\bar{B}$ ou $\bar{C}$. Comme p est un premier de bonne réduction, les décompositions de A, B et C restent les mêmes modulo p. Donc d'après ce qui précède, $\bar{x}$ est dans le support d'un certain $\bar{M}_\nu$: $\bar{x} \in \sup(\bar{M}_\nu)$. Donc $\bar{x} \in \sup(N\bar{M}_\nu) = \sup(\bar{m}_\nu^*(0))$. Donc $\bar{m}_\nu(\bar{x}) = \bar{0}$. On a vu que $\bar{f}(\bar{x}) = \bar{0} \Leftrightarrow v_p(f(x)) < 0$. On obtient ici $v_p(m_\nu(x)) < 0$.
On a $\bar{m}_\nu{}^*(\bar{0}) = N\bar{M}_\nu$; on admet que, de manière générale, $\operatorname{ord}_p(x)$ est un multiple de N. Donc ici, $v_p(m_\nu(x))$ est un multiple de $N \log p$.
Cela nous donne que $v_p(m_\nu(x)) = -\lambda N \log p,\ \lambda > 0$; le signe $-$ vient du fait que

$v_p(m_\nu(x))$ est négatif, mais N et $\log p$ sont positifs. Il vient alors :

$$\begin{aligned}\log p &= -\tfrac{1}{\lambda N} v_p(m_\nu(x)) \\ &\leq -\tfrac{1}{N} v_p(m_\nu(x)) \\ &\leq \sum_{\nu=1}^{k} \max(0, -\frac{1}{N} v_p(m_\nu(x))).\end{aligned}$$

Donc la contribution de p (c'est-à-dire $\log p$) au radical est bornée par :

$$\sum_{\nu=1}^{k} \max(0, -\frac{1}{N} v_p(m_\nu(x))).$$

On remarque pour la valuation v_∞ qu'on a bien :

$$0 \leq \sum_{\nu=1}^{k} \max(0, -\frac{1}{N} v_\infty(m_\nu(x))$$

car il s'agit d'une somme de termes positifs ou nuls : si $-\frac{1}{N} v_\infty(m_\nu(x)) < 0$, alors on prend 0. Cette somme est donc positive ou nulle.
On rappelle la définition du radical :

$$r(P) = r(a : b : c) = \sum_{p \,:\, \#\{v_p(a), v_p(b), v_p(c)\} \geq 2} \log p.$$

Donc ici :

$$\begin{aligned} r(P) &= \sum_{p \text{ de bonne réduction}} \log p \; + \sum_{p \text{ de mauvaise réduction}} \log p \\ &\leq \sum_{\text{bons } p} \sum_{\nu} \max(0, -\frac{1}{N} v_p(m_\nu(x)) + \sum_{\text{mauvais } p} \log p. \end{aligned}$$

On sait qu'il existe seulement un nombre fini de p de mauvaise réduction ; donc $\sum_{\text{mauvais } p} \log p$ est une somme finie, que l'on peut noter K_0.
De plus, on peut majorer la somme des valuations p-adiques pour p de bonne réduction par la somme de toutes les valuations, c'est-à-dire que l'inégalité ci-dessus devient :

$$r(P) \leq \sum_{\nu=1}^{k} \sum_{v} \max(0, -\frac{1}{N} v(m_\nu(x))) + K_0.$$

En considérant dans la suite uniquement l'ensemble des $m_\nu(x)$ avec $v(m_\nu(x)) < 0$ soit lorsque $-\frac{1}{N} v(m_\nu(x)$ est positif, notre inégalité devient :

$$\begin{aligned} \sum_{v} \max(0, -\frac{1}{N} v(m_\nu(x))) &= \sum_{v} -\frac{1}{N} v(m_\nu(x)) \\ &= \tfrac{1}{N} \sum_{v} - v(m_\nu(x)). \end{aligned}$$

On rappelle la définition de la hauteur :

$$h(P) = h(a : b : c) = \sum_{v} \max\{v(a), v(b), v(c)\}.$$

Ainsi, on obtient finalement :

$$\begin{aligned} r(P) &\leq \sum_{\nu=1}^{k}\sum_{v} \max(0, -\frac{1}{N} v(m_\nu(x))) + K_0 \\ &= \sum_{\nu=1}^{k} \frac{1}{N} h(m_\nu(x)) \ + K_0. \end{aligned} \qquad (*_{11})$$

On va maintenant majorer $h(m_\nu(x))$.
On sait que $\deg m_\nu = Nd_\nu$, et d'après $(*_6)$ dans la théorie des hauteurs :

$$|h_f(x) - h_g(x)| \leq K\sqrt{h_f(x)}$$

pour une certaine constante K et des fonctions $f, g : \mathcal{C} \to \mathbb{P}^1$.
En prenant $g = m_\nu$ on a, en considérant uniquement la borne inférieure :

$$\begin{aligned} |\tfrac{1}{d}h_f(x)) - \tfrac{1}{Nd_\nu}h(m_\nu(x))| &\leq K\sqrt{\tfrac{1}{d}h(f(x))} \\ h(x) - \tfrac{1}{Nd_\nu}h(m_\nu(x)) &\geq -K\sqrt{h(x)} \\ \tfrac{1}{Nd_\nu}h(m_\nu(x)) &\leq h(x) + K\sqrt{h(x)} \\ h(m_\nu(x)) &\leq Nd_\nu h(x) + Nd_\nu K\sqrt{h(x)}. \end{aligned}$$

On a majoré $h(m_\nu(x))$; on peut remplacer cette expression dans l'inégalité $(*_{11})$ et on obtient :

$$r(P) \leq \sum_{\nu=1}^{k} d_\nu h(x) + \sum_{\nu=1}^{k} d_\nu K\sqrt{h(x)} + K_0.$$

On peut noter $\displaystyle\sum_{\nu=1}^{k} d_\nu K = K_1$ et on a alors :

$$r(P) \leq \sum_{\nu=1}^{k} d_\nu h(x) + K_0 + K_1\sqrt{h(x)}.$$

On peut maintenant appliquer la conjecture ABC sous sa forme :

$$e(P) \leq \varepsilon h(P) + K_\varepsilon$$

avec $e(P) = \max(0, h(P) - r(P)) = h(P) - r(P)$.
On utilisera $(*_9)$ $\displaystyle\sum_{\nu=1}^{k} d_\nu = d + 2 - 2g$ et $(*_{10})$: $dh(x) \leq h(P)$.
La conjecture ABC nous donne donc :

$$\begin{aligned} h(P) - r(P) &\leq \varepsilon h(P) + K_\varepsilon \\ (1-\varepsilon)h(P) &\leq r(P) + K_\varepsilon \\ (1-\varepsilon)dh(x) &\leq r(P) + K_\varepsilon \\ dh(x) &\leq r(P) + \varepsilon dh(x) + K_\varepsilon. \end{aligned}$$

On pose $\varepsilon dh(x) + K_\varepsilon = \psi(dh(x))$, et on majore $r(P)$ par notre résultat précédent.

$$\begin{aligned} dh(x) &\leq \sum_{\nu=1}^{k} d_\nu h(x) + K_0 + K_1\sqrt{h(x)} + \psi(dh(x)) \\ (\sum_{\nu=1}^{k} d_\nu + 2g - 2)h(x) &\leq \sum_{\nu=1}^{k} d_\nu h(x) + K_0 + K_1\sqrt{h(x)} + \psi(dh(x)) \\ (2g-2)h(x) &\leq K_1\sqrt{h(x)} + K_0 + \psi(dh(x)). \end{aligned}$$

D'après $(*_4)$, $\psi(dh(x)) = o(h(x))$. De plus, comme $g \geq 2$, on a que $2g - 2 > 0$.
Ainsi, $h(x)$ est bornée. Or, d'après la théorie des hauteurs, pour tout $B > 0$, le nombre de $x \in \mathbb{P}^1(\mathbb{Q})$ avec $h(x) < B$ est fini. Donc ici, $\mathcal{C}(\mathbb{Q})$ est fini ce qui donne le résultat.

□

Chapitre 4

D'autres conséquences de la conjecture ABC

La conjecture ABC a énormément de conséquences, principalement dans la théorie des nombres. Nous venons de voir un exemple de son utilisation dans un domaine tout autre, mais nous allons ici nous pencher sur deux conséquences arithmétiques, où la manipulation de la conjecture est très simple, mais là où ses conséquences sont très importantes.

4.1 La conjecture d'Erdős-Woods

A) Introduction

Le problème est le suivant : existe-t-il un entier k tel que pour deux entiers x et y, si $\mathrm{Rad}(x+i) = \mathrm{Rad}(y+i)$ pour $i \in \{0, \dots, k\}$ alors $x = y$?
La conjecture ABC permet de donner des informations sur les valeurs possibles de k. En supposant la conjecture ABC vraie, cela va nous amener à des résultats assez intéressants.
Commençons par rappeler la conjecture ABC utile ici :

Conjecture ABC Soit $\epsilon > 0$. Il existe une constante C_ϵ tel que pour tout triplet $(a, b, c) \in \mathbb{Z}$ avec $\mathrm{pgcd}(a, b, c) = 1$ et $a + b = c$ alors :

$$\max(|a|, |b|, |c|) \leq C_\epsilon \,\mathrm{Rad}(abc)^{1+\epsilon}.$$

Nous allons utiliser la version de Baker $(*_1)$, avec $\varepsilon = \frac{3}{4}$:

$$\max(|a|, |b|, |c|) < \mathrm{Rad}(abc)^{\frac{7}{4}}.$$

Revenons au problème d'Erdős-Woods. On peut déjà remarquer que $k \neq 1$ par le théorème suivant :

Théorème 5 Il existe un nombre infini de couples d'entiers (x, y), avec $x < y$ vérifiant

$$\mathrm{Rad}(x) = \mathrm{Rad}(y) \text{ et } \mathrm{Rad}(x+1) = \mathrm{Rad}(y+1). \qquad (*_{12})$$

Démonstration. Soit $\gamma \geq 1$. On définit x et y comme suit :

$$x = 2^\gamma - 2 = 2(2^{\gamma-1} - 1) \text{ et } y = (2^\gamma - 1)^2 - 1 = 2^{\gamma+1}(2^{\gamma-1} - 1).$$

Nous avons $x + 1 = 2^\gamma - 1$ et $y + 1 = (2^\gamma - 1)^2$, donc :

$$\begin{array}{rcccl} \mathrm{Rad}(x) & = & \mathrm{Rad}(y) & = & 2\,\mathrm{Rad}(2^{\gamma-1} - 1) \\ \mathrm{Rad}(x+1) & = & \mathrm{Rad}(y+1) & = & \mathrm{Rad}(2^\gamma - 1) \end{array}$$

x et y vérifient donc bien $(*_{12})$. □

Remarque : Il existe un autre exemple ne suivant pas la forme ci-dessus, en prenant le couple suivant :

$$(x, y) = (75, 1215).$$

En effet :

$75 = 3 \times 5^2$ et $1215 = 3^5 \times 5$ donc $\mathrm{Rad}(75) = \mathrm{Rad}(1215) = 3 \times 5 = 15$.
$76 = 2^2 \times 19$ et $1216 = 19 \times 2^6$ donc $\mathrm{Rad}(76) = \mathrm{Rad}(1216) = 2 \times 19 = 38$.
Il n'y a pas d'autres exemples connus à ce jour.
De plus, personne n'a encore trouvé deux entiers x et y différents tels que $\mathrm{Rad}(x) = \mathrm{Rad}(y)$, $\mathrm{Rad}(x + 1) = \mathrm{Rad}(y + 1)$ et $\mathrm{Rad}(x + 2) = \mathrm{Rad}(y + 2)$. On en vient donc à la conjecture d'Erdős-Woods.

B) La conjecture d'Erdős-Woods

Conjecture 6 Il existe une constante absolue k tel que si x et y sont des entiers positifs satisfaisant $\mathrm{Rad}(x + i) = \mathrm{Rad}(y + i)$ pour $i \in \{0, 1, \cdots, k - 1\}$, alors $x = y$.

La conjecture ABC implique que cette conjecture est correcte pour $k = 2$, sauf pour un nombre fini de x.

Théorème 6 Si la conjecture ABC est vraie, alors il existe un nombre fini d'entiers $0 < y < x$ tel que

$$\begin{array}{c} \mathrm{Rad}(x) = \mathrm{Rad}(y), \\ \mathrm{Rad}(x+1) = \mathrm{Rad}(y+1), \\ \mathrm{Rad}(x+2) = \mathrm{Rad}(y+2). \end{array} \qquad (*_{13})$$

Démonstration. Prenons $y < x$ satisfaisant $(*_{13})$. On peut donc poser :

$$\begin{array}{ll} x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_u^{\alpha_u} & y = p_1^{\beta_1} p_2^{\beta_2} \dots p_u^{\beta_u} \\ x + 1 = q_1^{\gamma_1} q_2^{\gamma_2} \dots q_t^{\gamma_t} & y + 1 = q_1^{\zeta_1} q_2^{\zeta_2} \dots q_t^{\zeta_t} \\ x + 2 = r_1^{\delta_1} r_2^{\delta_2} \dots r_l^{\delta_l} & y + 2 = r_1^{\mu_1} r_2^{\mu_2} \dots r_l^{\mu_l}. \end{array}$$

On remarque :

$$\begin{aligned} p_j &\mid x-y, \\ q_i &\mid (x+1)-(y+1)=x-y, \\ r_h &\mid (x+2)-(y+2)=x-y. \end{aligned}$$

Appliquons la conjecture ABC aux trois équations suivantes :

$$\begin{aligned} \underbrace{x}_{a}+\underbrace{1}_{b} &= \underbrace{x+1}_{c} \\ \underbrace{(x+1)}_{a}+\underbrace{1}_{b} &= \underbrace{(x+2)}_{c} \\ \underbrace{x}_{a}+\underbrace{2}_{b} &= \underbrace{(x+2)}_{c} \end{aligned}$$

On a alors :

$$\begin{aligned} (x+1) &\leq C(\epsilon)\,\mathrm{Rad}(x(x+1)) = C(\epsilon)(\prod p_j \prod q_i)^{1+\epsilon} \\ (x+2) &\leq C(\epsilon)(\prod q_i \prod r_h)^{1+\epsilon} \\ (x+2) &\leq C(\epsilon)(2\prod p_j \prod r_h)^{1+\epsilon}. \end{aligned}$$

Dans le pire des cas, on peut avoir 2 comme facteur premier commun dans au plus deux des trois éléments x, $x+1$, et $x+2$, mais sinon les nombres premiers p_j,q_i et r_h sont distincts.

$$x^3 \leq (x+1)(x+2)^2 \leq C(\epsilon)^3(2\prod p_j \prod q_i \prod r_h)^{2+2\epsilon}.$$

Comme chaque p_j, q_i et r_h divise $x-y$ on a finalement que $\prod p_j \prod q_i \prod r_h | x-y$ d'où :

$$\begin{aligned} x^3 &\leq C(\epsilon)^3(2\prod p_j \prod q_i \prod r_h)^{2+2\epsilon} \\ x^3 &\leq C(\epsilon)^3(2(x-y))^{2+2\epsilon}. \end{aligned}$$

Comme $y < x$:

$$\begin{aligned} x^3 &\leq C(\epsilon)^3(2x)^{2+2\epsilon} \\ x^3 &\leq C(\epsilon)^3 2^{2+2\epsilon} x^{2+2\epsilon}. \end{aligned}$$

En prenant $\epsilon < \frac{1}{2}$ nous avons $2+2\epsilon < 3$ et :

$$\begin{aligned} x^{1-2\epsilon} &\leq C(\epsilon)^3 \times 2^{2+2\epsilon} \\ x &\leq C(\epsilon)^{\frac{3}{1-2\epsilon}} \times 2^{\frac{2+2\epsilon}{1-2\epsilon}}. \end{aligned}$$

Finalement, x est borné, ce qui nous donne un nombre fini de possibilités. □

On peut même aller plus loin. Dans un article publié par M. Langevin [6], ce dernier a montré en utilisant la forme explicite de la conjecture ABC donnée par A. Baker qu'il

existe un nombre fini d'exceptions à la conjecture d'Erdős-Woods pour le cas $k = 3$, avec cette fois-ci une borne effective.

Théorème 7 Si $0 < y < x$ sont deux entiers tels que :

$$\begin{aligned} \mathrm{Rad}(x) &= \mathrm{Rad}(y), \\ \mathrm{Rad}(x+1) &= \mathrm{Rad}(y+1), \\ \mathrm{Rad}(x+2) &= \mathrm{Rad}(y+2), \\ \mathrm{Rad}(x+3) &= \mathrm{Rad}(y+3), \end{aligned}$$

et si $(*_1)$ est vraie, alors $x < 6^7$.

Démonstration. Soient (x, y) avec $y < x$ vérifiant les hypothèses du théorème 7 :

$$\begin{aligned} x &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_u^{\alpha_u} & y &= p_1^{\beta_1} p_2^{\beta_2} \dots p_u^{\beta_u} \\ x+1 &= q_1^{\gamma_1} q_2^{\gamma_2} \dots q_t^{\gamma_t} & y+1 &= q_1^{\zeta_1} q_2^{\zeta_2} \dots q_t^{\zeta_t} \\ x+2 &= r_1^{\delta_1} r_2^{\delta_2} \dots r_l^{\delta_l} & y+2 &= r_1^{\mu_1} r_2^{\mu_2} \dots r_l^{\mu_l}. \\ x+3 &= s_1^{\omega_1} s_2^{\omega_2} \dots s_g^{\omega_g} & y+3 &= s_1^{\rho_1} s_2^{\rho_2} \dots s_g^{\rho_g}. \end{aligned}$$

Comme précédemment, on remarque :

$$\begin{aligned} p_j &\mid x - y, \\ q_i &\mid (x+1) - (y+1) = x - y, \\ r_h &\mid (x+2) - (y+2) = x - y, \\ s_m &\mid (x+3) - (y+3) = x - y. \end{aligned}$$

On applique $*_1$ aux deux équations suivantes :

$$x + 1 = (x + 1) \text{ et } (x + 2) + 1 = (x + 3)$$

pour obtenir :

$$\begin{aligned} (x+1) &\leq (\prod p_j \prod q_i)^{\frac{7}{4}} \\ (x+3) &\leq (\prod r_h \prod s_m)^{\frac{7}{4}}. \end{aligned}$$

Dans le pire des cas, 2 et 3 peuvent apparaitre deux fois, sinon les nombres sont tous distincts. En effet, si un premier p divise deux nombres différents a et b, alors $p|b - a$, donc dans notre cas p divise au plus 3.

$$\begin{aligned} x^2 \leq (x+1)(x+3) &\leq (\prod p_j \prod q_i \prod r_h \prod s_m)^{\frac{7}{4}} \\ &\leq (2 \times 3(x-y))^{\frac{7}{4}} \\ &\leq 6^{\frac{7}{4}} \times x^{\frac{7}{4}}. \end{aligned}$$

Finalement :

$$x \leq 6^7 = 279936$$

et on obtient une borne effective. □

4.2 Les premiers de Wieferich

Définition 4.1 (Premier de Wieferich)
Un nombre premier p est de Wieferich si $2^{p-1} \equiv 1 \ (mod\ p^2)$.

L'une des nombreuses conséquences de la conjecture ABC est la suivante :

Théorème 8 Soit p premier impair. Alors si la conjecture ABC est vraie, l'ensemble $U = \{p \ : \ 2^{p-1} \not\equiv 1 \ (mod\ p^2)\}$ est infini.

Démonstration. On raisonne par l'absurde.
Supposons que U est un ensemble fini. On pose $V = \{p \ : \ \text{p premier}, \ 2^{p-1} \equiv 1 \ mod\ (p^2)\}$ qui est l'ensemble des nombres de Wieferich.
Soit $n > 0$ entier, assez grand, tel que si $p_u \in U$, alors $p_u \nmid n$.
Nous allons étudier le nombre $2^n - 1$, qui est une suite non bornée. On l'écrit sous la forme $2^n - 1 = U_n V_n$, où les diviseurs premiers de U_n sont dans U et les diviseurs premiers de V_n sont dans V. On va chercher à montrer que les suites U_n et V_n sont bornées en utilisant notre hypothèse de départ, ce qui va mener à une contradiction car leur produit, $2^n - 1$, n'est pas borné.
On va montrer que

$$\begin{cases} p \mid U_n & \Longrightarrow \quad p^2 \nmid U_n, \\ p \mid V_n & \Longrightarrow \quad p^2 \mid V_n. \end{cases}$$

On pose $m_1 = o_p(2)$ et $m_2 = o_{p^2}(2)$, où $o_p(a)$ est l'ordre de a modulo p. Cela nous donne $2^{m_1} = 1 + \lambda p$, d'où

$$\begin{aligned} 2^{m_1 p} &= (1 + \lambda p)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} (\lambda p)^k \\ &\equiv 1 \ (mod\ p^2). \end{aligned}$$

D'où $m_1 p$ est un multiple de m_2 : $m_2 | m_1 p$.
D'autre part, on a que $2^{m_2} \equiv 1 \ (mod\ p^2) \Rightarrow 2^{m_2} \equiv 1 \ (mod\ p)$. Ce qui nous donne donc que m_2 est un multiple de m_1 : $m_1 | m_2$. Ainsi, on a soit $m_2 = m_1$, soit $m_2 = m_1 p$.

- On suppose que $p \mid U_n$.
  - Si $m_2 = m_1$, comme $m_1 | (p-1)$, on a que $m_2 | (p-1)$, et alors $2^{p-1} \equiv 1 \ (mod\ p^2)$. Mais $p \mid U_n \Longrightarrow p \in U$. Par définition, $2^{p-1} \not\equiv 1 \ (mod\ p^2)$. Il y a contradiction.
  - Donc $m_2 = m_1 p$, comme $p \in U$, on a $p \nmid n$, donc $m_2 \nmid n$. Donc $2^n \not\equiv 1 \ (mod\ p^2)$.

    On a montré que $p \mid U_n \Longrightarrow p^2 \nmid U_n$.

- On suppose que $p \mid V_n$.
  - Si $m_2 = m_1 p$, c'est impossible car $p | V_n \Longrightarrow p \in V$. Par définition, $2^{p-1} \equiv 1 \ (mod\ p^2)$; donc $m_2 | (p-1)$, $p \nmid n$: il y a une contradiction.

- Donc $m_2 = m_1$ et comme $p|V_n$, $p|(2^n - 1)$, $m_1|n$ car alors $2^n \equiv 1 \ (mod\ p)$. Donc comme $m_2 = m_1$, on obtient $m_2|n$, c'est-à-dire $2^n \equiv 1 \ (mod\ p^2)$, ou encore $p^2|(2^n - 1)$.

  On a montré $p \mid V_n \Longrightarrow p^2 \mid V_n$.

Posons maintenant $L := \prod_{p \in U} p$. On utilise ici l'hypothèse que U est fini, sinon L n'est pas fini. L est donc une constante.
Comme $p|U_n \Longrightarrow p^2 \nmid U_n$, $U_n = \prod_{p \mid U_n} p$ est sans facteur carré. D'où $U_n \leq L$.
D'autre part, comme $p|V_n \Longrightarrow p^2|V_n$, tous les facteurs de V_n sont au moins à la puissance 2. On obtient $\mathrm{Rad}(V_n) \leq {V_n}^{\frac{1}{2}}$.
On considère l'expression

$$(2^n - 1) + 1 = 2^n$$

c'est-à-dire $U_n V_n + 1 = 2^n$. Puis on lui applique la conjecture ABC :
D'une part, on a $V_n < U_n V_n + 1 = 2^n$,
D'autre part, on a par ABC : $\max(2^n - 1, 1, 2^n) \leq K_\epsilon \,\mathrm{Rad}((2^n - 1) \times 1 \times 2^n)^{1+\epsilon}$.

$$\begin{aligned} 2^n &\leq K_\epsilon \ \mathrm{Rad}(2^n U_n V_n)^{1+\epsilon} \\ &\leq K_\epsilon \ 2^{1+\epsilon} (\mathrm{Rad}(U_n) \ \mathrm{Rad}(V_n))^{1+\epsilon} \\ &\leq K_\epsilon \ 2^{1+\epsilon} \mathrm{Rad}(V_n)^{1+\epsilon} \ \mathrm{Rad}(U_n)^{1+\epsilon} \\ &\leq 2^{1+\epsilon} K_\epsilon \ \mathrm{Rad}(V_n)^{1+\epsilon} \ \mathrm{Rad}(U_n)^{1+\epsilon} \\ &\leq 2^{1+\epsilon} K_\epsilon {V_n}^{\frac{1+\epsilon}{2}} L^{1+\epsilon}. \end{aligned}$$

D'où $V_n \leq 2^{1+\epsilon} K_\epsilon {V_n}^{\frac{1+\epsilon}{2}} L^{1+\epsilon} \Longleftrightarrow V_n \leq (2^{1+\epsilon} K_\epsilon L^{1+\epsilon})^{\frac{2}{1-\epsilon}}$ (on peut supposer que $\epsilon \neq 1$ car ϵ peut prendre n'importe quelle valeur, donc on en choisit une en particulier, différente de 1). C'est une constante qui ne dépend pas de n, donc V_n est borné par rapport à n.Il y a donc contradiction : U est infini. □

Bibliographie

[1] Nils Bruin. Generalization of the abc-conjecture. Master's thesis, Leiden University, 1995. part. 1.2.

[2] Chambert-Loir. Théorèmes d'équidistribution pour les systèmes dynamiques d'origine arithmétique. In *Quelques aspects des systèmes dynamiques polynomiaux*, mai 2006.

[3] Henri Darmon and Andrew Granville. On the equations $z^m = f(x, y)$ and $ax^p + by^q = cz^r$. Preprint No. 28 Volume II, University of Georgia, 1994.

[4] Harold M. Edwards. *Fermat's last theorem.* Springer Verlag, 1977.

[5] Shanta Laishram and T.N. Shorey. Baker's explicit abc-conjecture and applications. *Acta Arithmetica*, 155(4), December 2011.

[6] Michel Langevin. Sur quelques conséquences de la conjecture (abc) en arithmétique et en logique. *Rocky Mountain J. Math.*, 26(3) :1031–1042, 1996.

[7] Brian Lawrence. Introduction to heights. Arithmetic Dynamics talk, April 2014.

[8] Joseph Sheppard. The abc conjecture and its applications. Master's thesis, B.A., Kansas State University, 2014.

[9] Machiel Van Frankenhuysen. Abc implies roth's theorem and mordell's conjecture. *Matematica Contemporanea 16*, pages 45–72, 1999.