Cours d'arithmétique M1, J-F. Mestre.

1 Formes quadratiques indéfinies et équation de Pell

THÉORÈME.- *Toute forme quadratique* (a, b, c) *à coefficients entiers est équivalente modulo* $\mathrm{SL}_2(\mathbf{Z})$ *à une forme vérifiant* $|b| \leq |a| \leq |c|$*; si* $D = b^2 - 4ac$ *est* > 0*, on a* $ac < 0$*, donc* $|b| < \sqrt{D}$*, donc il n'y a qu'un nombre fini de telles formes, et* $h(D)$*, le cardinal des formes quadratiques, à coefficients entiers premiers entre eux, de discriminant* D*, modulo l'action de* $\mathrm{SL}_2(\mathbf{Z})$*, est fini.*

CONJECTURE.- *Il y a une infinité de* $D > 0$ *tels que* $h(D) = 1$.

On s'intéresse plus particulièrement maintenant à la forme $x^2 - Dy^2$, $D > 0$ non carré.

PROPOSITION.- *Soit* $Q \geq 1$ *un entier, et* $x \in \mathbf{R}$*; il existe* p, q *premiers entre eux,* $1 \leq q \leq Q$*, tels que* $|x - \frac{p}{q}| \leq \frac{1}{qQ}$.

Démonstration par le principe des tiroirs de Dirichlet : on considère les $Q+1$ nombres $ix - [ix] \in [0, 1]$; il existe $i < j$ tels que $|ix - [ix] - (jx - [jx])| \leq 1/Q$, soit $|qx - p| \leq 1/Q$, avec $q = j - i$.

THÉORÈME. *Si* $D >$ *non carré, il existe une infinité de solutions entières de l'équation (dite de Pell)* $x^2 - Dy^2 = 1$*. Si* (x_0, y_0) *est la solution telle que* $x_0 > 0, y_0 > 0$*, et* $x_0 + y_0\sqrt{D}$ *minimal, les autres solutions sont celles obtenues à partir de* $\pm 1(x_0 + y_0\sqrt{D})^n$.

Si $x = \sqrt{D}$, on en tire que, pour tout Q, il existe p/q, $1 \leq q \leq Q$, tel que $|qx - p| \leq 1/Q$; pour Q assez grand, p est > 0, et $p \leq qx + 1/Q$, donc $p + qx \leq 2Qx + 1/Q$, d'où $|p^2 - q^2 D| \leq 2x + 1$; il existe donc une infinité de rationnels p/q tels que $|p^2 - q^2 x| \leq 2x + 1$; il existe donc $k \in \mathbf{Z}$ tel qu'il existe une infinité de p/q tels que $p^2 - q^2 D = k$; il existe donc α, β tels qu'il existe une infinité de p_i/q_i tels que $p_i \equiv p_j \mod k$ et $q_i \equiv q_j \mod k$. Soient deux d'entre elles; on a $(p_i - xq_i)(p_j + xq_j) = k^2(u + xv$ et $(p_i + xq_i)(p_j - xq_j) = k^2(u - xv)$, soit $k^2 = k^2(u^2 - Dv^2)$, et $u^2 - Dv^2 = 1$.

L'ensemble des solutions $p + qx > 0$ forme un groupe, discret (car si $x_n + y_n x$ tend vers 1, son inverse $x_n - xy_n$ aussi, donc x_n), donc de la forme $(p_0 + q_0 x)^n$.

EXEMPLE : la plus petite solution de $x^2 - 991y^2 = 1$ est

$$x = 379516400906811930638014896080, \quad y = 12055735790331359447442538767.$$

2 Fractions continues

1) Soit a_i, $i \geq 0$, une suite d'indéterminées. On pose

$$[a_0, a_1, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}}$$

$p_{-1} = 1,\ q_{-1} = 0,\ p_0 = a_0,\ q_0 = 1$, et

$$p_{n+1} = a_{n+1}p_n + p_{n-1}, \quad q_{n+1} = a_{n+1}q_n + q_{n-1}$$

pour $n \geq 1$.

Les p_n, q_n sont des éléments de $\mathbf{Z}[(a_i)]$, et les fractions $\frac{p_n}{q_n}$ s'appellent les *réduites* de la fraction continue $[a_o, \ldots]$; on a

Proposition.

- $p_{n-1}q_n - p_nq_{n-1} = (-1)^n$.
- $p_n/q_n - p_{n+1}/q_{n+1} = \frac{(-1)^{n+1}}{q_nq_{n+1}}$.
- $p_n/q_n = [a0, \ldots, a_n]$.
- *Si les a_i sont des entiers > 0, p_n et q_n sont des entiers premiers entre eux.*

Le point 3 se démontre par récurrence sur n: si la propriété demandée est vraie pour $n-1$, en posant $u_{n-1} = a_{n-1} + 1/a_n$, on a

$$[a0, \ldots, a_{n-2}, u_{n-1}] = \frac{u_{n-1}p_{n-2} + p_{n-3}}{u_{n-1}q_{n-2} + q_{n-3}} = \frac{p_{n-1} + \frac{p_{n-2}}{a_n}}{q_{n-1} + \frac{q_{n-2}}{a_n}} = \frac{p_n}{q_n}.$$

2) Soit $x \in \mathbf{R}$, et a_i, x_i les suites définies par $x_0 = x, a_i = [x_i], x_i = a_i + 1/x_{i+1}$ (si $x_i \neq a_i$).

Dans le cas où $x = p/q \in \mathbf{Q}$, on montre immédiatement par récurrence que $x_n = r_n/r_{n+1}$ et $p_nq - q_np = (-1)^nr_n$, les r_n et les a_n étant les restes et quotients successifs de Bezout de la division de p par q, pour $n \leq N$, où N est le plus petit n tel que tel que $r_{n+2} = 0$.

On suppose désormais $x \notin \mathbf{Q}$. Alors

Proposition.

- *Pour $n \geq 1$, on a $x_i > 1$, $a_i \geq 1$, (q_n) croissante.*
- $x = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}$.
- $x - p_n/q_n = \frac{(-1)^n}{q_n(q_nx_{n+1} + q_{n-1})}$.
- *La suite (p_n/q_n) est croissante (resp. décroissante) pour n pair (resp. impair); ces deux suites sont adjacentes, et tendent vers x.*
- *On a $|x - p_n/q_n| \leq \frac{1}{q_n^2}$ et, pour tout n, $|x - \frac{p_n}{q_n}| \leq \frac{1}{2q_n^2}$ ou $|x - \frac{p_{n+1}}{q_{n+1}}| \leq \frac{1}{2q_{n+1}^2}$.*

Théorème.- *Soit p, q tels que $q_n \leq q < q_{n+1}$. On a $|q_n x - p_n| \leq |qx - p|$, avec égalité ssi $(p, q) = (p_n, q_n)$.*

Soient $u, v \in \mathbf{Z}$ tels que $p = up_n + p_{n+1}$ et $q = uq_n + vq_{n+1}$; on a $uv \leq 0$, donc $|xq - p| = |u||xq_n - p_n| + |v||xq_{n+1} - p_{n+1}|$, d'où le résultat.

Théorème.- *Si p, q sont tels que $|x - p/q| < \frac{1}{2q^2}$, p/q est l'une des réduites de x.*

Soit n tel que $q_n \leq a < q_n$; on a

$$|pq_n - qp_n| = qq_n|p/q - p_n/q_n| \leq q_n|qx - p| + q|q_n x - p_n| \leq (q_n + q)|qx - p| < \frac{1}{q} \leq 1.$$

Remarque.- Les trois propositions précédentes restent vraies lorsque $x \in \mathbf{Q}$, $n \leq N$, N étant l'entier tel que x_{N+1} est un entier (et donc pour lequel x_{N+2} n'est plus défini.)

Théorème.- *Soit $a > 0$, $b > 0$ solutions de l'équation de Pell $a^2 - b^2 D = 1$; alors a/b est une réduite de $\sqrt{D}$.*

Si $x = \sqrt{D}$, on a $a > bx$, donc $|a - bx| = \frac{1|}{a+bx} < \frac{1}{2bx} < \frac{1}{2b}$.

Exemple.- Pour $D = 991$, la plus petite solution de l'équation de Pell écrite plus haut correspond à la 60-ième réduite de $\sqrt{991}$.

Théorème.- (Lagrange) *Une fraction continue est périodique à partir d'un certain rang ssi x est quadratique.*

Démonstration (du sens non trivial): soit $x = x_0$ quadratique, donc solution de $A_0 x^2 + B_0 x + C_0$, et $D = B_0^2 - 4A_0 C_0$; comme $x_n = a_n + \frac{1}{x_{n+1}}$, les x_n sont racines de $A_n x_n^2 + B_n x_n + C_n$, avec $B_n^2 - 4A_n C_n = B_0^2 - 4A_0 B_0 = D$, $C_{n+1} = A_n, B_{n+1} = B_n + 2a_n A_n$. Les A_n changent de signe une infinité de fois (sinon, si à partir d'un certain rang ils étaient par exemple > 0, les B_n seraient croissants, donc > 0 à partir d'un certain rang, C_n aussi, ce qui contredirait $x_n > 1$).

Donc il y a une infinité de n tels que $A_n A_{n+1} < 0$, soit $A_{n+1} C_{n+1} < 0$, d'où pour ces n $|B_n|$ borné par $\sqrt{D}$, d'où un nombre fini de A_n, B_n, C_n; donc il existe $m > n$ pour lequel $x_n = x_m$, cqfd.

Exemples: 1) le nombre d'or $\frac{1+\sqrt{5}}{2} = [1, 1, 1, \ldots]$, $\sqrt{2} = [1, 2, 2, 2, \ldots]$.

2) $\pi = [3, 7, 15, 1, 292, 1, 1, 1 \ldots]$, d'où

$$3, 22/7 = 3.142\ldots, 333/106 = 3.14150\ldots, 353/113 = 3.1415929\ldots$$

3) $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$

4) Huyghens et son automate planétaire:

Huyghens souhaitait construire, à l'aide d'un mécanisme de type horlogerie, un automate représentant le mouvement des planètes autour du soleil ; l'une des principales difficultés était due au rapport de la durée d'une année terrestre

et de celle de Saturne. En un an, la Terre tourne de $359^o45'40''30'''$ et Saturne de $12^o13'34''18'''$, d'où un rapport de 77708431/2640858. D'où la question : combien faut-il de dents sur les deux engrenages supportant respectivement la Terre et Saturne pour que le mouvement ne soit pas trop imprécis?

Huygens savait que les fractions continues offrent le meilleur compromis; Après calcul, on obtient $\frac{77\,708\,431}{2\,640\,858} = [29, 2, 2, 1, 5, 1, 4, 1, 1, 2, 1, 6, 1, 10, 2, 2, 3]$ d'où les réduites $29/1, 59/2, 147/5, 206/7, 1177/40\ldots$ Les deux premières solutions sont peu précises: dans le premier cas, à la fin d'une rotation de Saturne, la position de la terre est fausse de près d'un demi-tour, dans l'autre cas l'erreur dépasse 4°. La cinquième est techniquement difficile, elle demande la fabrication d'une roue à plus de 1 000 dents ou plusieurs roues. La quatrième offre une précision proche de 3/1 000. C'est celle que choisit Huygens.

Si la terre fait cent tours, sur l'automate planétaire Saturne en fait 700/206, soit trois tours et un angle de $143^o18'$. Dans la réalité, Saturne a tourné de $143^o26'$.

Soit une erreur de 8 minutes d'angle, largement inférieure aux imprécisions mécaniques de l'horloge. Un calcul analogue montre que la fraction 147/5 donne une erreur supérieure à un degré.

3 Approximation de nombres algébriques

Théorème.- (Liouville) *Soit x un nombre algébrique de degré $d \geq 2$; il existe $\alpha > 0$ tel que, pour tous p, q, on a*

$$|x - p/q| > \frac{\alpha}{q^d}.$$

Corollaire.- *Si x est tel qu'il existe une suite strictement croissante de nombres rationnels p_n/q_n tels que $|x - p_n/q_n| < 1/q_n^n$, alors x est transcendant.*

Exemple.- Pour tout $b \geq 2$,

$$\sum_{n \geq 0} b^{-n!}$$

est transcendant.

Théorème de Roth.- (admis) *Soit x un nombre algébrique de degré $d \geq 2$; pour tout $\varepsilon > 0$, il existe α tel que, pour tous p, q, on a*

$$|x - p/q| > \frac{\alpha}{q^{2+\varepsilon}}.$$