Université PIERRE ET MARIE CURIE 2009-2010
M1 Mathématiques Cryptographie

Devoir à la maison

Equations d'Hurwirtz

L'équation d'Hurwitz est

$$x_1^2 + \cdots + x_n^2 = kx_1 \cdots x_n, \quad n, k \in \mathbb{N}* \text{ avec } x_1, \cdots, x_n \in \mathbb{N}*.$$

1. Traiter les cas $n = 1$ et $n = 2$.
2. Montrer que si $(x_1, \cdots, x_n)$ est un solution de l'équation alors
$$(x_1, \cdots, x_{i-1}, x'_i, x_{i+1}, \cdots, x_n), \text{ avec} x'_i = kx_1 \cdots x_{i-1}x_{i+1} \cdots x_n - x_i$$
est aussi une solution.

On suppose désormais k et n fixés avec $n \geq 3$; on dira que deux solutions sont les mêmes si elles s'obtiennent l'une à partir de l'autre par permutation des indices. On ordonne ainsi les solutions $(x_1 \leq x_2 \leq \cdots \leq x_n)$ et on introduit la relation d'ordre lexicographique sur l'ensemble des solutions, i.e. $(x_1 \leq \cdots \leq x_n) < (y_1 \leq \cdots \leq y_n)$ si et seulement si $x_1 = y_1 \cdots x_k = y_k$ et $x_{k+1} < y_{k+1}$.

Définition : étant donnée une solution $(x_1, \cdots, x_n)$, les solutions de la question 2) sont dites voisines de $(x_1, \cdots, x_n)$; une solution sera dite fondamentale si elle est plus petite que toutes ses voisines.

3. Montrer qu'une solution possède au plus un père, i.e. un voisin qui lui est plus petit ; en déduire qu'une solution est associée à une unique solution fondamentale.
4. Montrer que si l'équation d'Hurwitz admet une solution alors elle en admet une infinité.

Une étude analytique à partir d'une solution minimale $(x_1 \leq \cdots \leq x_n)$ permet de montrer que $k \in \{1, \cdots, n\}$, ce que nous admettrons dans la suite. On s'intéresse désormais au cas $n = 3$.

5. Montrer qu'il y a une bijection entre les solutions associés au $k = 1$ avec celles associées à $k = 3$.

6. Montrer qu'il n'y a pas de solutions pour $k = 2$.

On s'intéresse désormais au cas $n = k = 3$ dont les solutions s'appellent des triplets de Markov ($x \leq y \leq z$) et les entiers z des nombres de Markov. Pour déterminer les solutions fondamentales qui permettent d'obtenir tous les nombres de Markov, par des majorations élémentaires on se ramène à tester un nombre fini de triplets. Finalement on trouve que $(1, 1, 1)$ est l'unique solution fondamental racine d'un arbre dit de Markov ; $(1, 1, 2)$ est l'unique fils et $(1, 2, 5)$ est l'unique petit fils.

7. Soit (x, x, y) un nombre de Markov ; montrer alors qu'à permutation près cette solution est $(1, 1, 2)$ ou $(1, 1, 2)$.
8. Soit $(x < y < z)$ un triplet de Markov ; montrer alors que cette solution a deux fils et un père.
9. Soit $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci. Montrer que pour tout $n \in \mathbb{N}$, F_{2n} est un nombre de Markov.

Une conjecture affirme qu'un nombre de Markov, n'apparait qu'une seule fois dans l'arbre, i.e. toute triplet de Markov ($x \leq y \leq z$) est déterminé par son élément maximal.

Définition : deux irrationnels θ et θ' sont dits équivalents s'il existe des entiers $a, b, c, d \in \mathbb{Z}$ tels que $|ad - bc| = 1$ et

$$\theta' = \frac{a\theta + b}{c\theta + d}.$$

Lagrange a montré qu'il existe une infinité d'approximation $\frac{p}{q}$ de θ telles que

$$|\theta - \frac{p}{q}| \leq \frac{1}{\sqrt{5}q^2}$$

et qu'on ne peut pas augmenter les $\sqrt{5}$ pour les irrationnels équivalents à $\theta = \frac{1+\sqrt{5}}{2}$. Pour tous les autres irrationnels, on a

$$|\theta - \frac{p}{q}| \leq \frac{1}{\sqrt{8}q^2}.$$

Définition : pour tout irrationnel x, on note

$$\nu(x) = \liminf_{q\to\infty} q \min_{p\in\mathbb{Z}} |qx - p|,$$

et $\lambda(c) = \nu(x)^{-1}$.

On peut montrer que ν est constant sur les classes d'équivalences d'irrationnels ; le théorème de Lagrange affirme alors que $\lambda(x) \geq \sqrt{5}$ avec égalité si et seulement si x est équivalent au nombre d'or ; pour les autres irrationnels on a $\lambda(x) \geq 2\sqrt{2}$ avec égalité si et seulement si x est équivalent à $\sqrt{2}$. La suite des valeurs prises par λ est alors

$$\lambda_m = \sqrt{9 - \frac{4}{m^2}}$$

où m décrit la suite des nombres de markov ; le cas d'égalité étant donné par la classe d'une solution de

$$mX^2 + (3m - 2q)X + (r - 3q)$$

où q est l'entier tel que m divise $q^2 + 1$ avec $0 < q < m/2$ et $r = \frac{q^2+1}{m}$.

Il y a encore de nombreux liens entre les nombres de Markov et les minima des formes quadratiques et les sommes de Dedekind.

Solutions

1) Pour $n = 1$, l'équation est $x_1^2 = kx_1$ et donc $x_1 = k$. Pour $k = 2$, en divisant l'équation homogène par $x_1 \wedge x_2$, on se ramène au cas $x_1 \wedge x_2 = 1$ et $x_1^2 + x_2^2 = kx_1x_2$ de sorte que $x_1 = x_2 = 1$ et $k = 2$.

2) Cela découle directement du fait que la somme des racines du polynôme $X^2 + a_1X + a_0$ vaut $-a_1$.

3) Soit $(u_1 \leq \cdots \leq u_n)$ l'un des pères de $(x_1 \leq \cdots \leq x_n)$ qui est donc égal à permutation près à $(x_1, \cdots, x_{i-1}, x'_i, x_{i+1}, \cdots, x_n)$ de sorte que $x'_i \leq x_i$ et donc

$$\begin{array}{lcl} x_i & \geq & kx_1 \cdots x_{i-1}x_{i+1} \cdots x_n - x_i \\ 2x_i & \geq & kx_1 \cdots x_{i-1}x_{i+1} \cdots x_n \\ 2x_i^2 & \geq & kx_1 \cdots x_n \\ 2x_1^2 & \geq & x_1^2 + \cdots + x_n^2 \\ x_i^2 & \geq & x_1^2 + \cdots + x_{i-1}^2 + x_{i+1}^2 + \cdots + x_n^2 \end{array}$$

de sorte que $i = n$ et donc $(u_1, \cdots, u_n)$ est une permutation de $(x_1, \cdots, x_{n-1}, x'_n)$ d'où le résultat.

Ainsi de père en père, en un nombre fini d'étapes, on ramène toute solution à une solution fondamentale.

4) Supposons par l'absurde qu'il n'y ait qu'un nombre fini de solutions ; l'ordre lexicographique étant total, il existe une solution maximale $(x_1 \leq \cdots \leq x_n)$. En reprenant les majorations de la question précédente, on obtient $x_1^2 \geq x_2^2 + \cdots + x_n^2$ ce qui est absurde vu que $n \geq 3$.

5) Modulo 3, si $x_i \not\equiv 0 \mod 3$ pour $i = 1, 2, 3$, on obtient $x_1x_2x_3 \equiv 1 + 1 + 1 \mod 3$ ce qui est contradictoire. Supposons $x_1 \equiv 0 \mod 3$, on trouve alors que $x_2 \equiv x_3 \equiv 0 \mod 3$ et donc

$$(\frac{x_1}{3})^2 + (\frac{x_2}{3})^2 + (\frac{x_3}{2})^2 = 3\frac{x_1}{3}\frac{x_2}{3}\frac{x_3}{3}.$$

6) x_1, x_2 et x_3 ne peuvent pas être pairs en même temps sinon on obtient une solution pour $k = 4$. En réduisant modulo 2, on trouve deux variables impaires et une paire ; $x_1 \equiv x_2 \equiv 1 \mod 2$ et $x_3 \equiv 0 \mod 2$. On obtient alors $2x_1x_2x_3 - x_3^2 = x_1^2 + x_2^2 \mod 4$ et donc $0 \equiv 2 \mod 4$, contradiction.

7) On a $2x^2+y^2=3x^2y$ et donc x divise y et $1+1+(\frac{y}{x})^2=(3x).1.1.(\frac{y}{c})$ et donc $k=3x$ ne peut être égal qu'à 1 ou 3 et donc $x=1$ et $2+y^2=3y$ et donc y divise 2 d'où le résultat.

8) On a $3xz-y=\frac{x^2+z^2}{y}>\frac{z^2}{z}=z$ et $3yz-x>3xz-y$ de sorte que $(x,z,3xz-y)$ et $(y,z,3yz-x)$ sont deux fils de (x,y,z) et donc $(x,y,3xy-z)$ est son unique père.

9) Si (x,y,z) est un triplet de Markov, alors (z,x_n,x_{n+1}) avec $x_{n+2}=3zx_{n+1}-x_n$ et $x_0=x$, $x_1=y$, est aussi un triplet de Markov. Il suffit alors de remarquer que $(1,1,1)$ est solution et que $F_{n+2}=F_{n+1}+F_n=3F_n-F_{n-2}$.

Corrigé