Spotting Patterns in Infinity Norms

EML Winter Semester 2023

Branch: Number Theory
Semester: 3 or 5
Language: English or French
Supervisors: Tim Seuré & Vincent Wolff
Contact: tim.seure@uni.lu & vincent.wolff@uni.lu

Goal of project

Fix an integer $n \geqslant 1$ and let $\omega_n := \exp(2\pi\mathrm{i}/n) \in \mathbb{C}$. Define the complex matrix $\boldsymbol{D}_n := \left(\omega_n^{ij}\right)_{i,j}$ with i and j running through $(\mathbb{Z}/n\mathbb{Z})^\times$ and $\{0, \ldots, \phi(n) - 1\}$, respectively.[1] For instance,

$$\boldsymbol{D}_4 = \begin{pmatrix} 1 & \omega_4^1 \\ 1 & \omega_4^3 \end{pmatrix}, \qquad \boldsymbol{D}_5 = \begin{pmatrix} 1 & \omega_5^1 & \omega_5^2 & \omega_5^3 \\ 1 & \omega_5^2 & \omega_5^4 & \omega_5^6 \\ 1 & \omega_5^3 & \omega_5^6 & \omega_5^9 \\ 1 & \omega_5^4 & \omega_5^8 & \omega_5^{12} \end{pmatrix}, \qquad \boldsymbol{D}_6 = \begin{pmatrix} 1 & \omega_6^1 \\ 1 & \omega_6^5 \end{pmatrix}.$$

Notice that $\boldsymbol{D}_n$ is a square matrix of size $\phi(n) \times \phi(n)$. It is not hard to show that $\boldsymbol{D}_n$ is invertible, and this allows us to consider its inverse matrix $\boldsymbol{D}_n^{-1}$. The goal of this project will be to better understand $d_n := \left\|\boldsymbol{D}_n^{-1}\right\|_\infty$, the infinity norm of $\boldsymbol{D}_n^{-1}$.[2]

Several results about the dependence of d_n on n are already known, and the first part of this project will be dedicated to understanding them. The ultimate goal would be to find a formula for (an upper bound on) d_n or to understand the asymptotic behavior of d_n. However, these objectives are likely too ambitious. Instead, we will already content ourselves with any kind of interesting conjecture in relation to d_n.

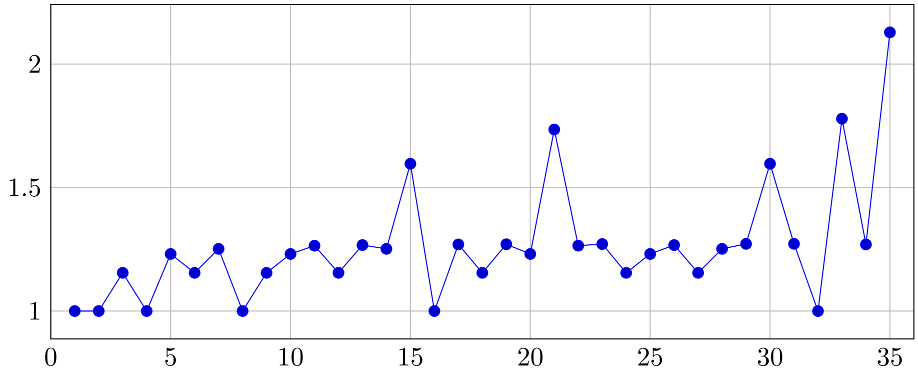

Figure 1: Plotting the points (n, d_n)

Figure 1 depicts the first few terms of the sequence $(d_n)_{n\geqslant 1}$. Can you already spot a pattern? For instance, can you guess for which n we have $d_n = 1$? And can you relate d_{2n} to d_n? Also, at which integers n will a new pike be reached? If these questions seem exciting, then this project is for you!

[1] Here, $\phi : \mathbb{N} \to \mathbb{N}$ denotes *Euler's totient function.*

[2] The *infinity norm* of a complex matrix $A = (a_{i,j})_{i,j}$ is defined to be $\|A\|_\infty := \max_i \sum_j |a_{i,j}|$.

Origin of problem

While this project will presumably be limited to the problem described above, we will now briefly explain where this problem actually originates from.

Various encryption schemes have their most important parts live in $\mathbb{R}$-algebras of the form $\mathscr{A}_n \coloneqq \mathbb{R}[X]/(\Phi_n)$.[3] Letting $x \coloneqq X + (\Phi_n) \in \mathscr{A}_n$, we can write $\mathscr{A}_n = \mathbb{R}[x]$, and elements $a \in \mathscr{A}_n$ can uniquely be written under the form $a = \sum_{0 \leqslant j < \phi(n)} a_j x^j$ with $a_j \in \mathbb{R}$. For such a, we can define

$$\|a\| \coloneqq \max_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} \left|a\big(\omega^i\big)\right|, \qquad \|a\|_{\mathsf{std}} \coloneqq \max_{0 \leqslant j < \phi(n)} |a_j|.$$

We then obtain two norms $\|\cdot\|$ and $\|\cdot\|_{\mathsf{std}}$ on $\mathscr{A}_n$, called the *canonical norm* and the *standard norm* on $\mathscr{A}_n$, respectively. Both have their own desirable properties. For instance, it is easy to show that the canonical norm is *sub-multiplicative*, which means that

$$\|ab\| \leqslant \|a\| \cdot \|b\|$$

for all $a, b \in \mathscr{A}_n$. Since all norms on finite-dimensional vector spaces are equivalent, there exist two real numbers $c, d > 0$ satisfying

$$c\|a\| \leqslant \|a\|_{\mathsf{std}} \leqslant d\|a\|$$

for every $a \in \mathscr{A}_n$. Being able to bound the standard norm in terms of the canonical one turns out to be the most useful in practice, and it is not hard to prove that we can choose $d \coloneqq d_n$.

[3] We denote by $\Phi_n \in \mathbb{Z}[X]$ the *n-th cyclotomic polynomial*.