TD n° 0 — Prise en main PARI/GP

Nomenclature officielle :

PARI/GP	le système complet,
PARI ou libpari	la bibliothèque,
gp	le calculateur, *i.e.* ce que vous utilisez,
GP	le langage utilisé pour programmer le calculateur.

Exercice 1
Consulter l'aide de la fonction `isprime`. Le nombre $2^{2^{11}} + 1$ est-il premier ?

Exercice 2
Consulter l'aide de la fonction `sigma`. Calculer la somme des carrés des diviseurs de $2^{128} + 1$.

Exercice 3
Le groupe $(\mathbb{Z}/42\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ est-il cyclique ?

Exercice 4
Consulter l'aide de la fonction `znstar`. Quelle est la structure de $(\mathbb{Z}/130\mathbb{Z})^\times$ en tant que groupe abélien ? Donner un système de générateurs pour ce groupe.

Exercice 5
1. Quel est le degré de l'extension $\mathbb{F}_8/\mathbb{F}_2$?
2. Quelle est la structure de $\mathbb{F}_8$ en tant que groupe abélien ?

Exercice 6
L'objectif de cet exercice est de rappeler la méthode d'exponentiation binaire.

1. Étant donné un entier naturel n, rappelons que son écriture en base 2 est de la forme
$$n = \sum_{i=0}^{k} \varepsilon_i 2^i$$
où $\varepsilon_i \in \{0, 1\}$ pour tout i. Écrire une procédure `base2`(n) qui renvoie la liste $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_k)$ des chiffres de n dans son écriture en base 2.
2. En déduire un algorithme d'exponentiation efficace dans un ensemble E muni d'une loi de multiplication $*$.
3. Le programmer pour $E = \mathbb{R}$. On appellera `puissance`(x, n) la procédure obtenue, qui, étant donné un réel x et un entier n, renvoie x^n.
4. Expliquer comment, grâce à Pari/gp, le même programme peut être utilisé dans $E = \mathbb{Z}/m\mathbb{Z}$ muni de la multiplication modulo m. Tester quelques exemples.