جامعة محمد الأول – وجدة
Université Mohammed Premier – Oujda
كلية العلـوم
Faculté des Sciences
شعبـة الرياضيات
Département de Mathématiques

Master de Théorie des Nombres

Semestre 2

PROGRAMMATION PARI/GP I

Les quatre TP de programmation PARI/GP I

Professeur : Moulay Chrif ISMAILI

Année Universitaire : 2019/2020

UNIVERSITÉ MOHAMMED I

FACULTÉ DES SCIENCES
DÉPARTEMENT DE MATHÉMATIQUES
O U J D A

Année Universitaire 2019/2020
Master de Théorie des Nombres
Semestre 2
Module : PARI/GP I

Premier TP de Programmation avec Pari

Exercice 1 Écrire le programme approprié pour dresser une liste des nombres premiers de la forme 2^p-1, en faisant varier p entre 2 et 607, évidemment p doit être un nombre premier. Afficher en même temps p et 2^p-1.

Exercice 2 Sachant que p désigne un nombre premier, en faisant varier p entre 2 et 19, calculer le reste de la division euclidienne de a^p-a par p lorsque a varie entre 1 et 19.

Exercice 3 Soit Le polynôme $P_m(X)=X^3-mX^2+(m^2-1)X+1$.
1) Imprimer les entiers $1<m<145$ pour lesquels $P_m(X)$ est irréductible.
2) Pour $m=5,11,13$, factoriser P_m modulo 7.

Exercice 4 Soit $n\in\mathbb{N}$ un entier naturel non nul qui n'est pas un cube. Soit $\mathbb{Q}(\sqrt[3]{n})$ le corps cubique pur défini par le polynôme X^3-n. On note $j=-1/2+i\sqrt{3}/2$ l'une des deux racines troisièmes de 1, (l'autre racine étant j^2). On rappelle que j est racine du polynôme X^2+X+1. On notera par $k=\mathbb{Q}(\sqrt[3]{n},j)$ le normalisé du corps cubique pur $\mathbb{Q}(\sqrt[3]{n})$. On sait que k est une extension diédrale de degré 6 sur $\mathbb{Q}$.
Dans toute la suite, $n=3p$ où p est un nombre premier tel que $p\equiv 1 \pmod 9$. On dit que 3 n'est pas un cube modulo p si pour tout entier a compris entre 1 et $p-1$, $3-a^3$ n'est pas divisible par p.
1) Déterminer tous les nombres premiers $p\equiv 1 \pmod 9$ tels que $5\leqslant p\leqslant 397$ et 3 n'est pas un cube modulo p.
2) Pour les premiers p trouvés dans la question précédente, vérifier que le nombre de classes de tous les corps cubiques purs $\mathbb{Q}(\sqrt[3]{3p})$ est exactement divisible par 3.

Exercice 5 Pour a et b des entiers naturels sans facteur carré tels que $2\leqslant a\leqslant 50$ et $1\leqslant b\leqslant 50$ et a et b premiers entre eux, écrire un programme qui donne le discriminant du polynôme x^3-ab^2 dans chacun des cas suivants :
1) $a\not\equiv\pm b \pmod 9$ et 3 premier avec ab.
2) $a\not\equiv\pm b \pmod 9$ et 3 divise ab.
3) $a\equiv\pm b \pmod 9$ et 3 premier avec ab.
Afficher en même temps a, b et le discriminant correspondant.

UNIVERSITÉ MOHAMMED I

Faculté Des Sciences
Département De Mathématiques
O u j d a

Année Universitaire 2019/2020
Master de Théorie des Nombres
Semestre 2
Module : PARI/GP I

Deuxième TP de Programmation avec Pari

Exercice 1 **1)** Écrire le programme approprié pour dresser une liste de tous les entiers $n \leqslant 10000$; de la forme $n = p_1 p_2 \cdots p_k$ où les p_i désignent des nombres premiers distincts deux à deux tel que $\forall i \in \{1, 2 \cdots, k\}$, $p_i - 1$ divise $n - 1$.
2) Vérifier que pour tout entier a premier avec n, on a :

$$a^{n-1} \equiv 1 \pmod{n}.$$

Les entiers vérifiant les propriétés citées dans **1)** s'appellent les nombres de Carmichaël.

Exercice 2 **1)** Écrire le programme approprié pour dresser une liste qui comporte l'unité fondamentale et le nombre de classes des corps quadratiques réels $\mathbb{Q}(\sqrt{d})$ lorsque d est sans facteur carré et d varie entre 2 et 1130.
2) Donner la liste de tous les entiers d tels que le nombre de classes du corps quadratique réel $\mathbb{Q}(\sqrt{d})$ soit :
a) exactement divisible par 2.
b) égal à 1.

Exercice 3 Soit $n \in \mathbb{N}$ un entier naturel non nul qui n'est pas un cube. Soit $\mathbb{Q}(\sqrt[3]{n})$ le corps cubique pur défini par le polynôme $X^3 - n$. On note $j = -1/2 + i\sqrt{3}/2$ l'une des deux racines troisièmes de 1, (l'autre racine étant j^2). On rappelle que j est racine du polynôme $X^2 + X + 1$. On notera par $k = \mathbb{Q}(\sqrt[3]{n}, j)$ le normalisé du corps cubique pur $\mathbb{Q}(\sqrt[3]{n})$. On sait que k est une extension diédrale de degré 6 sur $\mathbb{Q}$.
1) Écrire un programme qui permet de calculer le nombre de classes du corps cubique pur $\mathbb{Q}(\sqrt[3]{n})$ et du nombre de classes du normalisé k. Afficher le résultat en donnant n, le nombre de classes du corps cubique pur $\mathbb{Q}(\sqrt[3]{n})$ et le nombre de classes du normalisé k en faisant varier n entre 2 et 100.
2) Dans toute la suite, $n = 3p$ où p est un nombre premier tel que $p \equiv 1 \pmod{9}$, et 3 n'est pas un cube modulo p. Pour tous les premiers $5 \leqslant p \leqslant 397$ et 3 n'est pas un cube modulo p, donner la valuation modulo 3 du nombre de classes du corps cubique pur $\mathbb{Q}(\sqrt[3]{3p})$ et de son normalisé k.

UNIVERSITÉ MOHAMMED I
FACULTÉ DES SCIENCES
DÉPARTEMENT DE MATHÉMATIQUES
O U J D A

Année Universitaire 2019/2020
Master de Théorie des Nombres
Semestre 2
Module : PARI/GP I

Troisième TP de Programmation avec Pari

Exercice 1 **1)** Écrire le programme approprié pour dresser une liste de tous les nombres premiers $p \leqslant 100$ pour lesquels le nombre de classes du corps quadratique $\mathbb{Q}(\sqrt{p})$ est égal à 1.
2) Donner tous les nombres premiers p compris entre 2 et 2000 pour lesquels le nombre de classes de $\mathbb{Q}(\sqrt{p})$ est égal à 3, 5, 7, 9 ou 11.
3) Existe-t-il un polynôme normalisé, irréductible, de degré 5 et à coefficients dans $\mathbb{Z}$ tel que son discriminant soit égal à l'une des valeurs suivantes : -3, -4, -7, -8, -11, -19, -43, -67, -163 ou un nombre premier p tel que le nombre de classes de $\mathbb{Q}(\sqrt{p})$ est égal à 1 ?

Exercice 2 Calculer exactement les expressions algébriques suivantes dans les corps appropriés, où $n \in \mathbb{N}^*$:

$$A = \left(1+\sqrt{5}\right)^{10}, \quad B = \left(\sqrt[3]{19}^2+2\sqrt[3]{19}+19\right)^5, \quad C_n = \left(\frac{1+\sqrt{-3}}{2}\right)^{3n}.$$

Exercice 3 Montrer formellement l'identité :

$$\left(\frac{\frac{-1+\sqrt{5}}{2} + \sqrt{\frac{-\sqrt{5}-5}{2}}}{2} \right)^5 = 1.$$

UNIVERSITÉ MOHAMMED I

Faculté Des Sciences
Département De Mathématiques
O u j d a

Année Universitaire 2019/2020
Master de Théorie des Nombres
Semestre 2
Module : PARI/GP I

Quatrième TP de Programmation avec Pari

Exercice 1 Refaire le calcul de la formule

$$\left(\frac{\frac{-1+\sqrt{5}}{2} + \sqrt{\frac{-\sqrt{5}-5}{2}}}{2} \right)^5 = 1$$

en utilisant la commande rnfequation.

Exercice 2 Lorsque p est un nombre premier congru à 1 modulo 3, vérifier le critère d'Euler suivant :

$$\left(\frac{3}{p}\right)_3 = 1 \Leftrightarrow 3^{\frac{p-1}{3}} \equiv 1 \pmod{p}.$$

Exercice 3 **1)** Écrire les conditions qui permettent de vérifier qu'un entier n donné est libre de cube.

2) Soit $n \in \mathbb{N}$ un entier naturel non nul libre de cube. Soit $\mathbb{Q}(\sqrt[3]{n})$ le corps cubique pur défini par le polynôme $X^3 - n$. On note $j = -1/2 + i\sqrt{3}/2$ l'une des deux racines troisièmes de 1, (l'autre racine étant j^2). On notera par $k = \mathbb{Q}(\sqrt[3]{n}, j)$ le normalisé du corps cubique pur $\Gamma = \mathbb{Q}(\sqrt[3]{n})$, par h_k le nombre de classes de k et h_Γ celui de Γ. Déterminer le polynôme minimal définissant l'extension k moyennant la commande rnfequation.

3) En faisant varier n entre 2 et 998, vérifier que :

$$3h_k = h_\Gamma^2 \text{ ou } h_k = h_\Gamma^2.$$

4) Calculer les unités fondamentales de Γ et de k lorsque $3h_k = h_\Gamma^2$.

Exercice 4 On pose $n = 3p$ où p est un nombre premier tel que $p \equiv 1 \pmod 9$, et 3 n'est pas un cube modulo p. Pour tous les premiers $5 \leqslant p \leqslant 523$ et 3 n'est pas un cube modulo p, donner la valuation modulo 3 du nombre de classes du corps cubique pur $\Gamma = \mathbb{Q}(\sqrt[3]{3p})$, de son normalisé k et du corps $k(\sqrt[3]{p})$.