

Révision du 26 mai 2015 :

Nombres premiers - Théorème de GAUSS - Algorithme

EXERCICE 1

Pondichéry avril 2015

Les nombres de la forme $2^n - 1$ où n est un entier naturel non nul sont appelés **nombres de Mersenne**.

- 1) On désigne par a , b et c trois entiers naturels non nuls tels que $\text{pgcd}(b; c) = 1$.

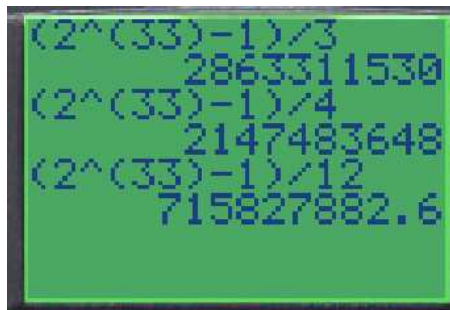
Prouver, à l'aide du théorème de Gauss, que :

si b divise a et c divise a alors le produit bc divise a .

- 2) On considère le nombre de Mersenne $2^{33} - 1$.

Un élève utilise sa calculatrice et obtient les résultats ci-dessous.

| | |
|------------------------|-------------|
| $(2^{33} - 1) \div 3$ | 2863311530 |
| $(2^{33} - 1) \div 4$ | 2147483648 |
| $(2^{33} - 1) \div 12$ | 715827882,6 |



Il affirme que 3 divise $(2^{33} - 1)$ et 4 divise $(2^{33} - 1)$ et 12 ne divise pas $(2^{33} - 1)$.

- En quoi cette affirmation contredit-elle le résultat démontré à la question 1) ?
 - Justifier que, en réalité, 4 ne divise pas $(2^{33} - 1)$.
 - En remarquant que $2 \equiv -1 \pmod{3}$, montrer que, en réalité, 3 ne divise pas $2^{33} - 1$.
 - Calculer la somme $S = 1 + 2^3 + (2^3)^2 + (2^3)^3 + \dots + (2^3)^{10}$.
 - En déduire que 7 divise $2^{33} - 1$.
- 3) On considère le nombre de Mersenne $2^7 - 1$. Est-il premier ? Justifier.
- 4) On donne l'algorithme, en annexe, où $\text{MOD}(N, k)$ représente le reste de la division euclidienne de N par k .
- Qu'affiche cet algorithme si on saisit $n = 33$? Et si on saisit $n = 7$?
 - Que représente le CAS 2 pour le nombre de Mersenne étudié ? Que représente alors le nombre k affiché pour le nombre de Mersenne étudié ?
 - Que représente le CAS 1 pour le nombre de Mersenne étudié ?

Annexe

Variables : n entier naturel supérieur ou égal à 3
 k entier naturel supérieur ou égal à 2

Entrées et initialisation

Demander à l'utilisateur la valeur de n
Affecter à k la valeur 2

Traitement et sorties

tant que $\text{MOD}(2^n - 1, k) \neq 0$ et $k \leq \sqrt{2^n - 1}$ **faire**

| Affecter à k la valeur $k + 1$

fin

Afficher k

si $k > \sqrt{2^n - 1}$ **alors**

| **Afficher** « CAS 1 »

sinon

| **Afficher** « CAS 2 »

fin