Asie Juin 2014

Partie A

• Le but de cette partie est de démontrer que l'ensemble des nombres premiers est infini, en raisonnant par l'absurde.

1. On suppose qu'il existe un nombre fini n de nombres premiers. notés $p_1, p_2, \dots, p_n$. On considère le nombre E produit de tous les nombres premiers augmenté de 1 :

$$E = p_1 \times p_2 \times \dots \times p_n + 1$$

Démontrer que E est un entier supérieur ou égal à 2, et que E est premier avec chacun des nombres $p_1, p_2, \dots, p_n$.

2. En utilisant le fait que E admet un diviseur premier, conclure.

Partie B

Pour tout entier naturel $k \geq 2$, on pose $M_k = 2^k - 1$. On dit que M_k est le k-iéme nombre de Mersenne.

1. *a*. Reproduire et compléter le tableau suivant, qui donne quelques valeurs de M_k.

k	2	3	4	5	6	7	8	9	10
M_k	3								

b. D'après k tableau précédent, si k est un nombre premier, peut-on conjecturer que le nombre M_k est premier?

2. Soient p et q deux entiers naturels non nuls.

a. Justifier l'égalité : $1 + 2^p + (2^p)^2 + ... + (2^p)^{q-1} = \dfrac{2^{pq} - 1}{2^p - 1}$

b. En déduire que $2^{pq} - 1$ est divisible par $2^p - 1$.

c. En déduire que, si un entier k supérieur ou égal à 2 n'est pas premier, alors M_k ne l'est pas non plus.

3. *a*. Prouver que le nombre de Mersenne M_{11} n'est pas premier.

b. Que peut-on en déduire concernant la conjecture de la question 1. *b*. ?

Partie C

Le test de Lucas-Lehmer permet de déterminer si un nombre de Mersenne donné est premier. Ce test utilise la suite numérique (u_n) définie par $u_0 = 4$ et, pour tout entier naturel n :

$$u_{n+1} = u_n^2 - 2$$

Si n est un entier naturel supérieur ou égal à 2, le test permet d'affirmer que le nombre M_n est premier si et seulement si $u_{n-2} \equiv 0$ modulo M_n. Cette propriété est admise dans la suite.

Utiliser le test de Lucas-Lehmer pour vérifier que le nombre de Mersenne M_5 est premier.

Soit n un entier naturel supérieur ou égal à 3.

L'algorithme suivant, qui est incomplet, doit permettre de vérifier si le nombre de Mersenne M_n est premier, en utilisant le test de Lucas-Lehmer.

Variables :	u, M, n et i sont des entiers naturels.
Initialisation :	u prend la valeur 4
Traitement :	Demander un entier $n \geq 3$ M prend la valeur …… Pour i allant de 1 à ……faire u prend la valeur ……… Fin Pour Si M divise u alors afficher « M ……………. » sinon afficher « M ……………. » FinSi

Recopier et compléter cet algorithme de façon à ce qu'il remplisse la condition voulue.

CORRECTION

Partie A

1. Le plus petit nombre premier est 2 donc $E \geq 2 + 1 \geq 2$

$E - p_1 \times p_2 \times \dots \times p_n = 1$, il existe donc deux entiers u et v tels que $u\,E + v\,p_1 = 1$ avec $1 \leq i \leq n$

D'après le théorème de Bézout, E est premier avec p_i pour $1 \leq i \leq n$

E est donc premier avec chacun des nombres $p_1, p_2, \dots, p_n$.

2. E n'est divisible par aucun nombre premier donc E est un nombre premier différent de tous les p_i, ce qui est contraire à l'hypothèse faite.

L'ensemble des nombres premiers est donc infini.

Partie B

1. *a*.

k	2	3	4	5	6	7	8	9	10
M_k	3	7	15	31	63	127	255	511	1023

***b*.** D'après le tableau, si k est premier (2, 3, 5 et 7), M_k l'est aussi. Si k est composé (non premier) M_k est composé.

La conjecture est donc qu'il y a une équivalence entre k est premier et M_k premier.

2. *a*. La somme $1 + 2^p + (2^p)^2 + ... + (2^p)^{q-1}$ à la somme des termes d'une suite géométrique de premier terme égal à 1 et de raison $b = 2^p$.

si $b \neq 1$ alors $1 + b + b^2 + \dots + b^{q-1} = \dfrac{b^q - 1}{b - 1}$. On a donc : $1 + 2^p + (2^p)^2 + ... + (2^p)^{q-1} = \dfrac{(2^p)^q - 1}{2^p - 1}$

b. $1 + 2^p + (2^p)^2 + ... + (2^p)^{q-1} = \dfrac{(2^p)^q - 1}{2^p - 1}$ donc $1 + 2^p + (2^p)^2 + ... + (2^p)^{q-1} = \dfrac{2^{pq} - 1}{2^p - 1}$

$2^{pq} - 1 = [1 + 2^p + (2^p)^2 + ... + (2^p)^{q-1}] \times [2^p - 1]$

$2^{pq} - 1$ est le produit de deux termes dont l'un est $2^p - 1$, il est donc divisible par ce nombre.

c. Si k est un entier supérieur ou égal à 2 non premier alors il existe 2 entiers p et q différents de 1 tels que $k = p\,q$.
Par conséquent $M_k = 2^k - 1 = 2^{pq} - 1$ donc M_k est divisible par $2^p - 1$ d'après la question précédente.
Pour montrer que M_k est premier, il faut de plus vérifier que $2^p - 1 \neq 1$ et $2^p - 1 \neq M_k$
$p \geq 2$ donc $2^p - 1 \geq 2^2 - 1$ donc $2^p - 1 \neq 1$
$2^p - 1 \neq M_k \Leftrightarrow 2^{pq} - 1 = 2^p - 1 \Leftrightarrow p = p\,q \Leftrightarrow p = 0$ ou $q = 1$ ce qui est exclu donc M_k admet un diviseur autre que 1 et lui-même donc M_k n'est pas premier.

a. $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ donc M_{11} n'est donc pas premier.

b. On a trouvé un nombre premier k pour lequel M_k n'est pas premier. La conjecture est donc fausse.

Partie C

$M_5 = 31$, $n = 5$ donc $n - 2 = 3$

n	0	1	2	3
u_n	4	14	194	37 634

$u_3 = 37634$ donc $u_3 = 31 \times 1214$ donc $u_3 \equiv 0$ modulo M_5.
Le test de Lucas-Lehmer fonctionne pour M_5.

Variables :	u, M, n et i sont des entiers naturels.
Initialisation :	u prend la valeur 4
Traitement :	Demander un entier $n \geq 3$ M prend la valeur $2^n - 1$ Pour i allant de 1 à $n - 2$ faire u prend la valeur $u^2 - 2$ Fin Pour Si M divise u alors afficher « M est un nombre premier » sinon afficher « M n'est pas un nombre premier » FinSi