Université de Metz
Département de Mathématiques

Année universitaire 2012-2013.

L3 Calcul formel

Feuille de TD n° 4

Exercice 1

Soit $n \in \mathbb{N}^*$. n est pseudo premier en base 2 si n est composé et si $2^n \equiv 2 \bmod n$. Le premier de ces nombres est 341=11×31. Le but de cet exercice est de montrer qu'il existe une infinité de nombres pseudo premiers en base 2.

1. Vérifier que 341 est un nombre pseudo premier en base 2.
2. Montrer que si n est pseudo premier en base 2 alors $2^n - 1$ divise $2^{2^n-1} - 2$.
3. Montrer que si n est composé alors $2^n - 1$ l'est aussi.
4. En déduire qu'il existe une infinité de nombres pseudo premiers en base 2.

Exercice 2

1. Montrer que 341 est pseudo premier en base 2 mais non en base 3.
2. Montrer que 91 est pseudo premier en base 3 mais non en base 2.

Exercice 3

Soit a un entier ≥ 2 et p un nombre premier impair ne divisant pas $a^2 - 1$.
Soit $n = \dfrac{a^{2p} - 1}{a^2 - 1}$.

1. Montrer que : $2/n - 1$, $p/a^{2p} - a^2$ et $p/n - 1$.
2. Montrer que : $2p/n - 1$ et $a^{2p} - 1/a^{n-1} - 1$.
3. Montrer que n est pseudo premier en base a.
4. Est ce que 341, qui est pseudo premier en base 2, est obtenu de cette façon ?
5. Montrer que le nombre d'entiers pseudo premiers en base a est infini.

Exercice 4 (Extraits du Capes 2003)

1. Soit p un nombre premier et a un entier premier avec p. Montrer que $a^{\frac{p-1}{2}}$ est congru à 1 ou $p - 1$ modulo p.
2. (a) Soit $n = \prod_{i=1}^{r} pi$ où p_1, p_2, ..., p_r sont des nombres premiers deux à deux distincts tels que $p_i - 1$ divise $n - 1$ pour tout $i \in 1, ..., r$. Montrer que n est un nombre de Carmichaël.

   (b) Application : montrer que 10585 est un nombre de Carmichaël.
3. Résoudre l'équation 85p -16q =1, où (p,q) $\in \mathbb{Z}^2$. Déterminer le plus petit nombre de Carmichaël divisible par 5 et 17.

Exercice 5

1. Montrer qu'un nombre de Carmichael est impair.
2. Soit p un nombre premier supérieur ou égal à 5 tel que $2p-1$ et $3p-2$ sont premiers. Montrer que $n = p.(2p-1).(3p-2)$ est un nombre de Carmichael.

Exercice 6

1. Calculer les symboles de Legendre $\left(\frac{26}{31}\right)$ et $\left(\frac{33}{37}\right)$.
2. Résoudre $x^2 + 7x - 2 \equiv 0 \mod 31$ puis $2x^2 + 5x - 1 \equiv 0 \mod 37$.

Exercice 7 Les nombres de Mersenne

1. Soit a un entier > 1. Montrer que si $a^n - 1$ est premier alors $a = 2$ et n est premier.

   Les nombres de la forme $2^p - 1$ où p est premier sont les **nombres de Mersenne**, notés M_p.
2. Calculer M_p pour $p = 2$, 3, 5, 7, 11 et 13.
3. D'après la question 1, la primalité de M_p nécessite celle de p. Cette condition est-elle suffisante ?
4. Le critère de primalité de Lucas-Lehmer se lit comme suit : " Soit p un nombre premier impair. Le nombre de Mersenne M_p est premier si et seulement si M_p divise S_{p-1} où $S_1 = 4$ et $S_{n+1} \equiv S_n^2 - 2\ [M_p]$".
   Etudier la primalité de M_{13}.
5. Soit p un nombre premier impair et soit q un diviseur premier du nombre de Mersenne M_p.
   (a) Montrer que $2^p \equiv 1\ [q]$. Quel est l'ordre de 2 modulo q ?
   (b) Montrer que $2^{q-1} \equiv 1\ [q]$. En déduire que q est de la forme $2kp + 1$, $k \in \mathbb{N}$.
   (c) Utiliser le (b) pour étudier la primalité du nombre de Mersenne M_{23}.
   (d) Utiliser le (b) pour étudier la primalité du nombre de Mersenne M_{17}.
6. Soit p un nombre premier tel que $p \equiv 3\ [4]$.
   Montrer que $2p + 1$ est premier si et seulement si $2p + 1$ divise M_p.
7. Montrer que si m et n sont des entiers premiers entre eux alors M_m et M_n sont également premiers entre eux.

Exercice 8

Tester la primalité de 1729 :

1. en utilisant le test de Fermat,
2. en utilisant le test de Miller-Rabin,
3. en utilisant le test de Solovay-Strassen.

Exercice 9

Soient a et b des entiers >1.

1. Montrer que si a est un résidu quadratique modulo b alors $\left(\frac{a}{b}\right) = 1$.
2. La réciproque est-elle vraie ?