Université de Paris-Sud 2005

Math 102, L1 et L2

Feuille d'exercices n°3

1. Les nombres $2^{456}+7$ et 15 sont-ils premiers entre eux?

2. Montrer que $2^{70}+3^{70}$ est divisible par 13.

3. Montrer que pour tout entier naturel n, $2^{2^{6n+2}}+3$ est divisible par 19.

4. Montrer que $20^{15}-1$ est divisible par 20801.

5. Montrer qu'il existe dans la suite $u_n = 2^n - 3$ une infinité de termes divisibles par 5 et une infinité de termes divisibles par 13, mais qu'aucun n'est divisible par 65.

6. Soit $p = 2k+1$ un nombre premier impair. Soit a un entier non divisible par p. Montrer que $a^k \equiv 1$ ou $a^k \equiv -1$ modulo p. Application numérique : faire le tableau des restes des puissances huitièmes modulo 17.

7. Montrer que si n est un entier naturel impair, alors 10^n+1 est divisible par 11. En déduire que le nombre 1 343 113 431 est divisible par 121.

Montrer que si n est un entier naturel impair, alors $10^{3n}+1$ est divisible par 13. En déduire que le nombre 169 169 000 169 169 est divisible par 13^4.

8. Soient a et b deux entiers strictement positifs premiers entre eux, et soit $n > 1$ un autre entier.

1. Soit p un facteur premier de a^n+b^n, qui ne divise aucun des a^m+b^m pour m divisant n et distinct de n. Montrer que, alors, $p \equiv 1\,(2n)$
2. Soit p un facteur premier de a^n-b^n, qui ne divise aucun des a^m-b^m pour m divisant n et distinct de n. Montrer que, alors, $p \equiv 1\,(n)$. Montrer que si n est impair, on a même $p \equiv 1\,(2n)$.

9. Il s'agit d'une méthode pour partager un secret s entre 3 personnes, qui soit toujours reconstituable par 2 quelconques d'entre elles, et inaccessible à une quelconque d'entre elles.

On distribue 3 informations partielles $(I_i)_{1\leq i\leq 3}$ sur le secret s. Montrer qu'il existe 3 nombres premiers m_1, m_2, m_3 tels que

1. $m_1 < m_2 < m_3$
2. $m_1 m_2 > m_3$

On pourra choisir les m_i dans un intervalle de la forme $]p^{\frac{2^2-1}{2^2}}, p]$, où p est un nombre premier suffisamment grand pour que cet intervalle contienne 3 nombres premiers. On définit: $M = m_1 m_2$ et $N = m_3$ et on code le secret s par un nombre tel que $N \leq s \leq M$.

On distribue à chaque personne P_i le nombre I_i, $0 \leq I_i \leq m_i - 1$ où $I_i \equiv s\,(m_i)$.

Vérifier que la donnée de 2 des (I_i) permet de reconstituer s: appliquer le théorème chinois et le fait que $s \leq M$. Vérifier que la connaissance de un seul des (I_i) détermine s modulo un nombre inférieur à N, donc donne $\frac{M-N}{N}$ valeurs possibles de s.

Généraliser au cas où l'on partage un secret s entre n personnes, qui soit toujours reconstituable par k quelconques d'entre elles, et inaccessible à une coalition de $k-1$ quelconque d'entre elles.

10. Protocole d'échange de messages.
Alice et Bob veulent échanger des messages sans que le contenu puisse être lu par quelqu'un qui les intercepterait. Ils se mettent d'accord sur un nombre premier p (qui peut éventuellement être connu de tout le monde). Si Alice veut envoyer le message M à Bob, où M est un entier avec $0 \leq M < p$, voici ce qu'ils font :
1) Alice choisit un entier a premier avec $p-1$, puis calcule un entier a' tel que $aa' \equiv 1\ (p-1)$. Elle garde a et a' secrets.
2) Bob fait de même pour avoir deux entiers b, b' tels que $bb' \equiv 1\ (p-1)$. Il garde b et b' secrets.
3) Alice calcule $C_1 \equiv M^a\ (p)$ avec $0 \leq C_1 < p$ et envoie C_1 à Bob.
4) Bob calcule $C_2 \equiv (C_1)^b\ (p)$ avec $0 \leq C_2 < p$ et envoie C_2 à Alice.
5) Alice calcule $C_3 \equiv (C_2)^{a'}\ (p)$ avec $0 \leq C_3 < p$ et envoie C_3 à Bob.
6) Bob calcule $C_4 \equiv (C_3)^{b'}\ (p)$ avec $0 \leq C_4 < p$.

Montrer que $C_4 = M$.

Ce protocole d'échange s'appelle "protocole des valises" par analogie avec la situation suivante : Alice met le message dans une valise et met un cadenas dont elle seule a la clé (c'est a). Bob reçoit la valise, met un autre cadenas (b) et renvoie la valise à Alice. Alice ouvre son propre cadenas (a') et renvoie la valise. Bob peut alors ouvrir la valise en ouvrant son propre cadenas (b'). La valise est toujours fermé quand elle voyage.