Année universitaire 2013-2014
Licence 3 de mathématiques
Cryptographie et arithmétique - Feuille 2

Exercice 1 : algorithme de Karatsuba

Posons $\alpha = \log_2 3$. Soit n un entier ≥ 1.

a. Soient a et b deux entiers naturels $< 2^{2n}$. Comment calculer ab en n'effectuant que trois multiplications d'entiers naturels $< 2^n$ (*indication :* écrire $a = 2^n a_1 + a_2$ et $b = 2^n b_1 + b_2$ puis considérer $(a_1 + a_2)(b_1 + b_2)$) ?

b. Soient a et b deux entiers naturels $< 2^n$. Proposer un algorithme donnant ab de complexité $O(n^\alpha)$.

Exercice 2

a. Calculer l'inverse de $\bar{25}$ dans l'anneau $\mathbb{Z}/37\mathbb{Z}$.

b. Quels sont les éléments inversibles de l'anneau $\mathbb{Z}/12\mathbb{Z}$?

Exercice 3

a. Trouver tous les entiers n vérifiant $2n \equiv 5 \bmod 21$.

b. Trouver tous les $x \in \mathbb{Z}/25\mathbb{Z}$ vérifiant $\bar{20}x = \bar{15}$.

c. Trouver tous les couples $(x; y) \in \mathbb{Z}^2$ vérifiant : $x + y \equiv 6 \bmod 11$ et $2x - y \equiv 8 \bmod 11$.

Exercice 4 : algorithme d'Euclide binaire

Soient a et b deux entiers tels que $1 \leq b \leq a$.

a. Montrer que si a et b sont impairs, alors $a \wedge b = \dfrac{a-b}{2} \wedge b$.

b. Proposer un algorithme donnant le pgcd de a et b en n'effectuant que s soustractions (et des divisions par 2), avec $s \leq \log_2(a + b)$.

Exercice 5

Trouver tous les entiers n vérifiant : $2n \equiv 3 \bmod 5$ et $3n \equiv 1 \bmod 7$.

Exercice 6

a. Montrer que si m est un entier impair, alors $m^2 \equiv 1 \bmod 8$.

b. Soient a, b, c trois entiers. Montrer que $a^2 + b^2 + c^2$ n'est pas congru à 7 modulo 8.

Exercice 7

Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également, et de donner le reste au cuisinier. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et 6 d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Survient alors un naufrage, et seuls 6 pirates, le trésor et le cuisinier sont sauvés. Le partage laisserait 5 pièces d'or à ce dernier. Il décide alors d'empoisonner les autres survivants. Quelle est la fortune minimale que peut espérer le cuisinier ?

Exercice 8

Soit n un entier.

a. Soient p un nombre premier et r un entier naturel. Montrer que p divise $n^{pr-r+1} - n$.

b. En déduire que 2730 divise $n^{13} - n$.

Exercice 9

On note $(F_n)_{n\geq 0}$ la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$, et $F_{n+2} = F_{n+1} + F_n$ pour tout $n \geq 0$.

a. Montrer que F_n et F_{n+1} sont premiers entre eux pour tout $n \geq 0$.

b. Soient m et n deux entiers tels que $1 \leq m \leq n$. Montrer la relation $F_n = F_m F_{n-m+1} + F_{m-1} F_{n-m}$.

c. En déduire que $F_m \wedge F_n = F_{m \wedge n}$ pour tout $(m; n) \in \mathbb{N}^{*2}$.

Exercice 10 : complexité de l'algorithme d'Euclide

On désigne par $(F_n)_{n\geq 0}$ la suite de Fibonacci. Soient a et b deux entiers ≥ 1. Le but de cet exercice est de borner le nombre m de divisions effectuées par l'algorithme d'Euclide appliqué à a et b.

a. Montrer que $F_{m+1} \leq b$ (*indication :* remonter l'algorithme).

b. Posons $\varphi = \dfrac{1+\sqrt{5}}{2}$. Vérifier que $F_n \geq \varphi^{n-2}$ pour tout $n \geq 1$. En déduire la majoration $m \leq \dfrac{\ln b}{\ln \varphi} + 1$.

Exercice 11 : critère de Pépin

Soit n un entier naturel ; on pose $E_n = 2^{2^n} + 1$.

a. Soit p un facteur premier de E_n. Déterminer l'ordre de $\bar{2}$ dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$. En déduire que 2^{n+1} divise $p-1$.

b. Supposons qu'il existe un entier a tel que $a^{(F_n-1)/2} \equiv -1 \bmod E_n$. En s'inspirant de la question **a**, montrer que E_n est premier.

Exercice 12

Soient n et a deux entiers ≥ 2. Montrer que n divise $\varphi(a^n - 1)$.