Feuille d'exercices 6.

Exercice 1 Soit $p = F_n = 2^{2^n} + 1$ un nombre de Fermat premier. Montrer que $x \in (\mathbb{Z}/p\mathbb{Z})^*$ est un générateur si et seulement si il n'est pas un carré. En utilisant la loi de la réciprocité quadratique, montrer que 3, 5, 7 sont des générateurs de $(\mathbb{Z}/p\mathbb{Z})^*$ pour $n \geq 2$. En déduire le critère de Pépin: $p := F_n$ est premier si et seulement si $3^{(p-1)/2} = -1 \bmod p$.

Exercice 2 Utiliser le test de Fermat pour trouver que le cinquième nombre de Fermat $F_5 = 2^{2^5} + 1$ est composé. Prouver que tous les nombres de Fermat sont pseudo-premiers pour la base 2.

Exercice 3 Soit n un entier naturel impair et soit b un entier premier à n.
a) Montrer que si p est un diviseur premier de n, et si on pose $n' = n/p$, alors n est pseudo-premier pour la base b implique que $b^{n'-1} = 1 \bmod p$.
b) Prouver qu'il n'y a pas d'entier de la forme $n = 3p$ (ou $p > 3$ est premier) qui soit pseudo-premier pour les bases 2, 5 et 7.
c) Prouver qu'il n'y a pas d'entier de la forme $n = 5p$ (ou $p > 3$ est premier) qui soit pseudo-premier pour les bases 2, 5 et 7.
d) Prouver que 91 est le plus petit nombre pseudo-premier pour la base 3.

Exercice 4 On veut utiliser le test de Solovay-Strassen pour tester si 451 est un nombre premier:
1) On décide de faire ce test en au plus 3 itérations. Pour cela on doit choisir a chaque itération une valeur aléatoire. Dans quel intervalle doit-on choisir cette valeur?
2) On choisit au hasard successivement les valeurs 373, 59 et 161. Faire le test de Solovay-Stassen avec ces valeurs. Combien d'itération avez-vous effectuées? A chaque itération donner la probabilité d'erreur qu'on obtiendrait si on arêtait le test?

Exercice 5 (Nombres pseudo-premiers forts, extrait Capes 2003) Dasn cet exercice, p désigne un nombre premier impair supérieur ou égal à 3, et on notera $(p-1) = q \times 2^s$, où q est un entier naturel impair et s un entier naturel supérieur ou égal à 1.
1) Dans cette question on suppose p premier. On dit qu'un entier naturel a vérifie la propriété $H_a(p)$ si:

$$(a^q = 1 \bmod p) \text{ ou } (\exists r \text{ entier}, 0 \leq r < s \text{ tel que } a^{q \times 2^r} = p - 1 \bmod p) \qquad (H_a(p))$$

Montrer que tout entier naturel a premier avec p vérifie $H_a(p)$.
2) On dit qu'un nombre p impair, non nécessairement premier, est pseudo-premier fort en base a si la propriété $H_a(p)$ est vérifiée: on écrira en abrégé que p est a-ppf.

Par exemple, 25 est 7-ppf car $24 = 3 \times 2^3$ et $7^{3\times 2} = 117649 = 24 = -1 \bmod 25$.

Montrer que si a est un entier tel que le pgcd de a et p est strictement plus grand que 1, alors p ne peut pas être a-ppf.
3) Construction d'un algorithme:
a) Un entier p impair et un entier a étant donnés, écrire un algorithme permettant de tester si p est a-ppf.
b) Compléter le tableau suivant:

p	49	91	111	121	135	1225
a	30	74	28	94	43	999
p est $a - ppf$						

Exercice 6 (Attaque $p-1$ sur RSA)
Cette attaque est très performante lorsque p (un des facteurs du module $N = pq$) possède une propriété particulière: soit B un entier arbitraire (qu'on choisira petit); on dit qu'un nombre est B-lisse si tous ses diviseurs premiers sont inférieurs ou égaux à B.
1) Montrer que l'ensemble des nombres B-lisses est stable par multiplication.

L'attaque dite $p-1$ fonctionne si $p-1$ est B-lisse (pour un B quelconque que l'on supposera connu). Elle se base sur le théorème de Fermat et le calcul de pgcd.

2) Rappeler comment s'écrit le petit théorème de Fermat dans $\mathbb{Z}/p\mathbb{Z}$.
3) En déduire que pour tout a premier avec p, et tout entier k multiple de $p-1$, on a $pgcd(a^k-1, N) \neq 1$.
4) Expliquer comment construire simplement un (grand) multiple de $p-1$, en utilisant la B-lissité. (Rappel: la valeur de p est inconnue)
5) Conclure.

Exercice 7 (Examen Janvier 2008) Pour factoriser l'entier $n = 24961$ en utilisant la méthode du crible quadratique, on considère la base de factorisation $B = \{-1, 2, 3, 5, 13, 23\}$.
1) Expliquer pourquoi on a exclu les nombres $\{7, 11, 17, 19\}$ de la base B.
2) On rappelle que $157 < \sqrt{24961} < 158$. Utiliser le tableau suivant pour la factorisation de n, en se servant de l'indication qui suit:
On cherche une relation de dépendance linéaire entre les vecteurs v_i. Les relations $v_2 + v_4 + v_5 = 0$ et $v_5 + v_6 + v_7 = 0$ n'aboutiront pas à une solution.

a_i	$a_i^2 \bmod n$	b_i	$v_i \in (\mathbb{F}_2)^6$
151	-2160	$-2^4.3^3.5$	$v_1 = (1,0,1,1,0,0)$
155	-936	$-2^3.3^2.13$	$v_2 = (1,1,0,0,1,0)$
156	-625	-5^4	$v_3 = (1,0,0,0,0,0)$
157	-312	$-2^3.3.13$	$v_4 = (1,1,1,0,1,0)$
158	3	3	$v_5 = (0,0,1,0,0,0)$
159	320	$2^6.5$	$v_6 = (0,0,0,1,0,0)$
161	960	$2^6.3.5$	$v_7 = (0,0,1,1,0,0)$