TD 7. Tests de primalité

Exercice 1
Pour quels entiers b l'entier 6 est-il probablement premier de base b ?

Exercice 2
On rappelle que l'*exposant* d'un groupe fini G est le ppcm des ordres des éléments de G, et que l'*indicateur de Carmichael* d'un entier m est l'exposant $\lambda(m)$ de $(\mathbb{Z}/m\mathbb{Z})^*$.

a) Vérifier que l'exposant de G est le plus petit entier e tel que $x^e = 1$ pour tout $x \in G$.

b) Montrer qu'un entier n est probablement premier de base b pour tout entier b premier à n si et seulement si $\lambda(n)$ divise $n-1$.

c) On a $561 = 3 \times 11 \times 17$. Vérifier que $\lambda(561)$ divise 560 ; de plus, on donne :

$$2^{140} \equiv 67 \mod 561 \quad \text{et} \quad 2^{280} \equiv 1 \mod 561 \ .$$

Le nombre 561 est-il probablement premier fort de base 2 ?

Exercice 3

a) On donne $3^6 = 729$ et $728 = 8 \times 91$; en déduire que 91 est probablement premier de base 3. On donne $2^{12} = 4096$ et $4095 = 45 \times 91$; 91 est-il probablement premier de base 2 ? Conclusion ?

b) Montrer que 121 est fortement probablement premier de base 3, sachant que $3^5 = 243$; de même pour 781 en base 5, sachant que $5^5 - 1 = 4 \times 781$. Ces deux nombres sont-ils premiers ?

c) On donne :

$$2^{14} = 16\,384 \ , \quad 16\,383 = 3 \times 5461 \ , \quad 5460 = 14 \times 390 = 4 \times 1365 \ , \quad 1365 = 14 \times 97 + 7 \ .$$

Montrer que 5461 est-il probablement premier de base 2. Est-il fortement probablement premier de base 2 ?

d) Faire de même pour 7381 en base 3, sachant que $3^{10} - 1 = 8 \times 7381$, et pour 105 en base 13, sachant que $13^4 - 1 = 272 \times 105$.

e) On donne :

$$2^{16} - 1 = 15 \times 4369 \ , \quad 4368 = 16 \times 273 \ , \quad 273 = 16 \times 17 + 1 \ .$$

Montrer que 4369 est pseudo premier de base 2.

Exercice 4 (Un nouveau test de primalité)

1. Soient $\varphi > 0$ et $\bar{\varphi} < 0$ les racines de $X^2 - X - 1$.

   a) Déterminer le discriminant de $X^2 - X - 1$ et une expression de φ et $\bar{\varphi}$; calculer $\varphi\bar{\varphi}$ et $\varphi + \bar{\varphi}$.

b) On raisonne dans l'anneau d'entiers $\mathbb{Z}[\varphi]$ de $\mathbb{Q}(\sqrt{5})$. Montrer que, pour p premier impair, $2\varphi^p \equiv (2\varphi)^p \mod p$ est congru à $1+\varepsilon\sqrt{5}$ modulo p, où $\varepsilon = \left(\frac{5}{p}\right)$ est le symbole de Legendre de 5 sur p.

c) en déduire que $\varphi^{p-\varepsilon} \equiv \bar{\varphi}^{p-\varepsilon} \equiv \varepsilon \mod p$.

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

   a) Montrer que, pour tout entier n, on a

$$F_n = \frac{\varphi^{n+1} - \bar{\varphi}^{n+1}}{\varphi - \bar{\varphi}} = \varphi^n + \varphi^{n-1}\bar{\varphi} + \varphi^{n-2}\bar{\varphi}^2 + \cdots + \varphi\bar{\varphi}^{n-1} + \bar{\varphi}^n \ .$$

   b) Soit p un premier impair tel que $\varepsilon = \left(\frac{5}{p}\right) = 1$, montrer que p divise F_{p-2} (noter que $\frac{1}{\varphi-\bar{\varphi}} = \frac{\sqrt{5}}{5}$).

   c) Soit p un premier impair tel que $\varepsilon = \left(\frac{5}{p}\right) = -1$, montrer que p divise F_p.

   Noter qu'on a $F_4 = 5$ donc p divise F_{p-1} si $\left(\frac{5}{p}\right) = 0$.

3. On dit qu'un entier impair n est *probablement premier de Fibonacci* si n divise $F_{n-1-\varepsilon}$, où $\varepsilon = \left(\frac{5}{n}\right)$ est le symbole de Jacobi de 5 sur n.
   Calculer les symboles de Jacobi de 5 sur 323 et 377 et vérifier que ces deux nombres sont *pseudo-premiers de Fibonacci*[1].

Comme dans le test basé sur le théorème de Fermat, il existe une version forte de ce test (que 323 et 377 ne passent pas ; 4181 et 5777 la passent) ; par ailleurs, on peut construire des tests similaires en remplaçant la suite de Fibonacci par une *suite de Lucas*, donnée par $V_0 = 2$, $V_1 = P$ et, pour $n \geq 0$:

$$V_{n+2} = PV_{n+1} - QV_n \ ,$$

où P, Q sont des entiers tels que $D = P^2 - 4Q$ ne soit pas un carré.

[1] $F_{323} = 23\,041\,483\,585\,524\,168\,262\,220\,906\,489\,642\,018\,075\,101\,617\,466\,780\,496\,790\,573\,690\,289\,968$,
$F_{377} = 4\,444\,705\,723\,234\,237\,498\,833\,973\,519\,982\,908\,519\,933\,430\,818\,636\,409\,166\,351\,397\,897\,095\,281\,987\,215\,864$.