COMPLEX - PROJET

Tests de primalité

Fatemeh Hamissi
Kim-Anh Laura Nguyen
Promo 2018-2019

Chargé de TP : Alexandre Teiller

2. Test naïf et recherche des nombres de Carmichael

a)

```
def first_test(n):
    '''
        n : entier
        effectue le test naÃ¯f de primalitÃ© sur n
    '''
    if n<7:
        if n in (2,3,5):
            return True
        else:
            return False
    if n & 1 == 0:
        return False
    k=3
    r=math.sqrt(n)
    while k<=r:
        if n % k == 0:
            return False
        k+=2
    return True
```

b) `first_test` est exponentiel en la taille de l'entrée.

c)
d)
f)

g) Montrons qu'il n'existe qu'un nombre fini de nombres de Carmichael de la forme pqr avec $p < q < r$ trois nombres premiers pour p fixé.

1. Soit n un nombre de Carmichael de la forme pqr avec $p < q < r$ trois nombres premiers. Montrons qu'il existe un entier $h \in \{2, ..., p-1\}$ tel que $(pq-1) = h(r-1)$.

Démonstration.
D'après le critère de Korselt, on a :

$$p-1 \mid pqr-1$$
$$q-1 \mid pqr-1$$
$$r-1 \mid pqr-1$$

d'où

$$p-1 \mid qr-1$$
$$q-1 \mid pr-1$$
$$r-1 \mid pq-1$$

et l'on peut écrire qu'il existe trois entiers l, k, h tels que,

$$qr-1 = l(p-1) \tag{1}$$
$$pr-1 = k(q-1) \tag{2}$$
$$pq-1 = h(r-1) \tag{3}$$

et l'on a bien $(pq-1) = h(r-1)$. De plus, q et r ne peuvent pas être consécutifs car premiers, d'où $q < r-1$. On a alors $qh < pq$ et donc $h < p$. Comme h et p sont des entiers, on obtient $h \leq p-1$. On a aussi $h > 1$ car $pq-1 \neq r-1$ car $pq \neq r$ car r est premier. Donc $h \in \{2, ..., p-1\}$.

□

2. Montrons qu'il existe un entier k tel que

$$(hk - p^2)(q-1) = (p+h)(p-1) \tag{4}$$

Démonstration.

D'après l'équation 2, il existe k tel que $pr - 1 = k(q-1)$. On a donc

$$\begin{aligned} k(q-1) &= pr - 1 \\ &= p(r-1) + (p-1) \\ &= p\,\frac{pq-1}{h} + (p-1) \\ &= \frac{p}{h}\,(pq-1) + (p-1) \end{aligned}$$

d'où

$$\begin{aligned} hk(q-1) &= p(pq-1) + h(p-1) \\ hkq - hk &= p^2q - p + hp - h \end{aligned}$$

et

$$\begin{aligned} (hk-p^2)(q-1) &= (p+h)(p-1) \\ hkq - hk - p^2q + p^2 &= p^2 - p + hp - h \\ hkq - hk - p^2q &= -p + hp - h \\ hkq - hk &= p^2q - p + hp - h \end{aligned}$$

donc il existe un entier k tel que $(hk - p^2)(q-1) = (p+h)(p-1)$.

□

3. Montrons qu'il n'existe qu'un nombre fini de nombres de Carmichael avec 3 facteurs premiers.

Démonstration.

Soit p un nombre premier. Notons $f(p)$ le nombre de nombres de Carmichael à 3 facteurs premiers dont le plus petit est p.

Soit h tel que $2 \leq h \leq p-1$. Une fois $hk - p^2$ fixé, q est déterminé par l'équation 4 et r par l'équation 3. On obtient alors

$$hk - p^2 = \frac{(p+h)(p-1)}{q-1} \geq 1$$

De plus, comme $p < q$, on a $p-1 < q-1$ et donc $hk - p^2 < p+h$, soit $hk - p^2 \leq p+h-1$. On obtient alors $1 \leq hk - p^2 \leq p+h-1$. Pour p et h fixés, $hk - p^2$ prend donc ses valeurs dans un intervalle de taille $p+h-2$.

De plus, on doit avoir $hk - p^2 \equiv -p^2 \mod h$. Chaque intervalle de taille h contient donc une seule valeur possible pour $hk - p^2$.

On obtient donc le nombre de choix suivant pour $hk - p^2$,

$$\frac{p+h-2}{h} + 1 = \frac{p-2}{h} + 2$$

Finalement,

$$f(p) \leq \sum_{h=2}^{p} (\frac{p-2}{h} + 2) < (p-2)(\log p + 2)$$

□