Corrigé
Arithmétique : nombres premiers

Déterminer si un nombre est premier

Exercice 1.

1. Les nombres 221, 223 et 391 sont-ils premiers ?
2. À l'aide du crible d'Ératosthène, dresser la liste des nombres premiers inférieurs à 100.
3. Combien de nombres premiers inférieurs à 100 y a-t-il ?

1. $221 = 13 \times 17$ non premier ; 223 n'est divisible par aucun premier $\leqslant 14$ (2, 3, 5, 7, 11, 13) : premier ; $391 = 17 \times 23$ non premier.
2. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.
3. 25.

Exercice 2. [Algorithme]

1. Compléter la fonction Python `est_premier(n)` qui teste les diviseurs d tels que $d^2 \leqslant n$.

```
def est_premier(n):
    if n < 2:
        return False
    d = 2
    while d * d <= n:
        if n % d == ...:
            return False
        d = d + 1
    return ...
```

2. Écrire une fonction `liste_premiers(N)` qui renvoie la liste des nombres premiers inférieurs ou égaux à N.

1. `if n % d == 0:` et `return True`.
2. `def liste_premiers(N): return [n for n in range(2, N + 1) if est_premier(n)]`

Décomposer un nombre en produit de facteurs premiers

Exercice 3.

1. Décomposer en produit de facteurs premiers : 252, 1 008, 2 026, 1 001.
2. Déterminer le plus petit entier naturel k tel que $252k$ soit un carré parfait.
3. $\sqrt{1\,008}$ s'écrit $a\sqrt{b}$ avec a, b entiers et b le plus petit possible : déterminer a et b.

1. $252 = 2^2 \times 3^2 \times 7$; $1\,008 = 2^4 \times 3^2 \times 7$; $2\,026 = 2 \times 1\,013$ (1 013 est premier) ; $1\,001 = 7 \times 11 \times 13$.
2. Il faut des exposants pairs : $k = 7$ ($252 \times 7 = 1\,764 = 42^2$).
3. $1\,008 = (2^2 \times 3)^2 \times 7$: $\sqrt{1\,008} = 12\sqrt{7}$.

Déterminer les diviseurs d'un entier et en déduire un PGCD

Exercice 4.

1. Combien 252 a-t-il de diviseurs positifs ? Les lister.
2. Calculer PGCD(252 ; 1 008) et PGCD(252 ; 2 026) à l'aide des décompositions.
3. Simplifier la fraction $\dfrac{252}{1\,008}$.

1. $3 \times 3 \times 2 = 18$ diviseurs : 1, 2, 3, 4, 6, 7, 9, 12, 14, 18, 21, 28, 36, 42, 63, 84, 126, 252.
2. PGCD(252 ; 1 008) = 252 (car $1\,008 = 4 \times 252$) ; PGCD(252 ; 2 026) = 2.
3. $\dfrac{252}{1\,008} = \dfrac{1}{4}$.

Utiliser le petit théorème de Fermat

Exercice 5.

1. Déterminer le reste de la division euclidienne de 2^{100} par 11.
2. Déterminer le reste de 5^{2026} dans la division par 13.
3. Montrer que pour tout entier n, $n^7 - n$ est divisible par 7, puis par 42.

1. 11 premier ne divise pas 2 : $2^{10} \equiv 1$ [11], donc $2^{100} = (2^{10})^{10} \equiv 1$ [11].
2. $5^{12} \equiv 1$ [13] ; $2026 = 12 \times 168 + 10$; $5^{2026} \equiv 5^{10}$ [13]. Or $5^2 \equiv -1$, donc $5^{10} \equiv (-1)^5 = -1 \equiv 12$ [13].
3. Fermat : $n^7 \equiv n$ [7]. De plus $n^7 - n = n(n^6 - 1) = n(n-1)(n+1)(n^2+n+1)(n^2-n+1)$ contient $n(n-1)(n+1)$, divisible par 2 et par 3. 2, 3, 7 sont premiers entre eux deux à deux : 42 divise $n^7 - n$.

Exercice 6. [Chiffrement RSA simplifié]

On choisit $p = 5$, $q = 11$, $n = pq = 55$ et $e = 3$. Un message M (entier de 0 à 54) est chiffré en $C \equiv M^3$ [55].

1. Chiffrer $M = 2$ et $M = 8$.
2. Vérifier que $3 \times 27 \equiv 1$ [40], avec $40 = (p-1)(q-1)$.
3. On admet que pour tout M, $M^{81} \equiv M$ [55] (conséquence du petit théorème de Fermat appliqué à 5 et 11). En déduire que $C^{27} \equiv M$ [55], puis déchiffrer $C = 17$.

1. $2^3 = 8$; $8^3 = 512 = 55 \times 9 + 17$, donc $C = 17$.
2. $81 = 2 \times 40 + 1$.
3. $C^{27} \equiv M^{81} \equiv M$ [55]. Pour $C = 17$, on retrouve $M = 8$ (question 1). La calculatrice confirme : $17^{27} \equiv 8$ [55].