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 ?

Exercice 2. [Algorithme]

1. Compléter la fonction Python $\text{est_premier}(\text{n})$ 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 $\text{liste_premiers}(\text{N})$ qui renvoie la liste des nombres premiers inférieurs ou égaux à 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.

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 $\dfrac{252}{1\,008}$.

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.

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 $C = 17$.

Corrigé