Plaquette 5 – Synthèse : PGCD, PPCM par décomposition et cryptographie

Nombres premiers — Terminale maths expertes

Exercices

Méthode

La plaquette de synthèse : on lit **PGCD et PPCM directement dans les décompositions**, on compte les facteurs premiers d'une factorielle, on découvre les **nombres parfaits**, et l'on met tout le chapitre au service d'un **chiffrement RSA** miniature — la raison pour laquelle les nombres premiers font tourner Internet.

Exercice 1 – PGCD et PPCM par décomposition

a) Décomposer 504 et 1 188 en facteurs premiers.

b) En déduire leur PGCD et leur PPCM.

c) Vérifier la relation pgcd × ppcm = ab.

Exercice 2 – Trois nombres à la fois

Déterminer pgcd(600 ; 540 ; 1 050) et ppcm(600 ; 540 ; 1 050).

Exercice 3 – Retrouver un entier

Déterminer tous les entiers naturels n tels que pgcd(n ; 504) = 36 et $n \leq 200$.

Exercice 4 – Combien de zéros à la fin ?

a) Par combien de zéros se termine l'écriture décimale de 100 ! ?

b) Même question pour 2 026 !.

Exercice 5 – L'exposant d'un premier dans une factorielle

a) Déterminer l'exposant de 3 dans la décomposition de 20 !.

b) 20 ! est-il divisible par 3^9 ?

Exercice 6 – La somme des diviseurs

a) Calculer la somme des diviseurs de 28, puis de 496.

b) Que remarque-t-on ? Vérifier avec 6.

Exercice 7 – Construire une clé RSA

On choisit $p = 5$ et $q = 11$, puis $n = pq$ et $\varphi = (p-1)(q-1)$.

a) Calculer n et φ.

b) On prend $e = 3$. Vérifier que e est premier avec φ, puis déterminer d tel que $ed \equiv 1 \pmod{\varphi}$.

Exercice 8 – Chiffrer et déchiffrer

On reprend la clé publique $(n\,;e) = (55\,;3)$ et la clé privée $d = 27$.

a) Chiffrer le message $m = 7$ par $c \equiv m^{3} \pmod{55}$.

b) Déchiffrer le résultat par $m \equiv c^{27} \pmod{55}$.

Exercice 9 – Casser une clé trop petite

Une clé publique est $(n\,;e) = (55\,;3)$.

a) Expliquer comment un attaquant retrouve la clé privée.

b) Pourquoi cette attaque est-elle impossible en pratique avec les vraies clés RSA ?

Exercice 10 – Un produit imposé

Déterminer tous les couples d'entiers naturels $(a\,;b)$ avec $a \leq b$ tels que $ab = 2\,520$ et $\text{pgcd}(a\,;b) = 6$.

Exercice 11 – Une fraction et ses facteurs

a) Rendre irréductible $\dfrac{2\,520}{1\,188}$ en passant par les décompositions.

b) Déterminer le plus petit entier $k \geq 1$ tel que $\dfrac{2\,520}{k}$ soit un entier **impair**.

Exercice 12 – Des cartes à distribuer

Un jeu comporte 504 cartes. On veut les répartir en paquets identiques, chaque paquet contenant entre 20 et 80 cartes.

a) Quelles tailles de paquets sont possibles ?

b) Combien 504 a-t-il de diviseurs au total ?

Exercice 13 – Deux roues et un PPCM

Deux satellites d'observation ont des périodes de révolution de 540 minutes et 600 minutes. Ils sont alignés au-dessus d'une station à midi.

a) Au bout de combien de temps seront-ils de nouveau alignés au-dessus de la station ?

b) Combien de révolutions chacun aura-t-il accomplies ?

Exercice 14 – Un code de vérification

Un identifiant a est transformé en $c \equiv a^{5} \pmod{23}$ (on rappelle que 23 est premier).

a) Coder l'identifiant $a = 4$.

b) Montrer que la transformation est inversible et donner l'exposant de déchiffrement.

Exercice 15 – Bilan : tout le chapitre

a) Décomposer $1\,050$ et $2\,520$, puis donner leur PGCD, leur PPCM et le nombre de diviseurs de $2\,520$.

b) Déterminer le reste de 6^{2026} dans la division par 17.

c) Un cryptosystème utilise $n = 35$ et $e = 5$. Déterminer la clé de déchiffrement d, puis déchiffrer le message $c = 3$.