Arithmétique : nombres premiers
Problème de recherche : le test de primalité de l'ordinateur

Pour créer des clés de chiffrement (comme pour les paiements par carte bancaire), un ordinateur doit trouver de très grands nombres premiers. Il ne peut pas tester tous les diviseurs : c'est beaucoup trop long. Il utilise donc ce test :

> **Test de Fermat en base 2.** Pour un entier impair $n \geqslant 3$, on calcule le reste de 2^{n-1} dans la division par n. Si ce reste vaut 1, l'ordinateur déclare : « n est premier » ; sinon : « n n'est pas premier ».

La mission

1. Expliquer pourquoi le test ne se trompe jamais quand il déclare « n n'est pas premier ».
2. Appliquer le test à $n = 91$, sans calculer 2^{90} en entier.
3. Appliquer le test à $n = 341$. Le test peut-il se tromper ?

Pour aller plus loin

Appliquer à 341 le même test en base 3 (reste de 3^{340} modulo 341). Qu'en penser ?

Coups de pouce

Bloqué ? Des indices progressifs sont disponibles en ligne. N'en ouvrir qu'un à la fois, et seulement après avoir cherché !