FICHE 06

Nombres premiers et théorème de Fermat

Primalité ▪ Factorisation ▪ Puissances

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30

Les briques de la multiplication

Terminale — Option Mathématiques expertes — Programme officiel

Cours · 15 exercices · Problème guidé · Corrigés

Table des matières

1 Pourquoi ce chapitre ?

1.1 Le problème fondamental : retrouver les briques d'un entier

$60 = 6 \times 10 = 4 \times 15$ possède plusieurs produits possibles. En décomposant jusqu'aux nombres premiers, tu retrouves toujours $2^2 \times 3 \times 5$, à l'ordre près. Cette stabilité rend la factorisation utile pour compter les diviseurs, reconnaître les carrés ou comparer deux entiers.

Intuition | Deux questions, deux outils

« Quels facteurs contient ce nombre ? » appelle une décomposition. « Quel est le reste de cette grande puissance ? » appelle des congruences et, sous ses hypothèses, Fermat. Il est essentiel de choisir la question avant de lancer un calcul.

Prérequis. Division euclidienne, congruences, PGCD, Bézout et Gauss. Savoir distinguer une implication de sa réciproque est particulièrement important pour les tests de primalité.

Méthode | Objectifs

Tester la primalité de petits entiers ; démontrer l'infinitude des nombres premiers ; utiliser l'unicité de la factorisation ; appliquer Fermat avec ses hypothèses ; écrire des algorithmes exacts.

L'énoncé de Fermat appartient au programme. Sa preuve par permutation et l'application RSA sont des prolongements guidés ; ils utilisent exclusivement les outils construits dans ces fiches.

Méthode | Comment travailler cette fiche

Commence par l'idée avant la formule, puis travaille une notion à la fois. Dans le cours, reformule la définition avec tes mots et refais l'exemple sans regarder la dernière ligne. Les pauses te proposent une question, deux indices graduels et une explication ; tu peux chercher avec une aide sans renoncer au raisonnement.
Après le cours, la boîte à outils relie plusieurs notions dans des méthodes commentées. Les exercices passent des bases aux questions d'initiative. Si tu bloques, prends d'abord un indice ; après le corrigé, explique pourquoi la méthode convient et refais une variante. Le problème final construit un approfondissement à partir du cours, puis une dernière activité te permet de faire le point.

2 L'idée avant la formule

2.1 Pourquoi arrêter les essais à la racine carrée ?

Si $n = ab$ avec $1 < a \leq b$, le plus petit facteur vérifie $a^2 \leq ab = n$. Dans chaque paire de facteurs, l'un se trouve donc avant ou sur la racine carrée. Pour 91, tester jusqu'à 9 suffit : le facteur 7 révèle $91 = 7 \times 13$. La borne inclut les carrés, comme 49 et son facteur 7.

2.2 L'unicité transforme un dessin de facteurs en preuve

Un arbre de décomposition suggère les facteurs premiers. Pour assurer que deux arbres donnent la même liste, nous utiliserons Gauss : un premier qui divise un produit doit diviser l'un de ses facteurs. C'est ce résultat qui permettra de comparer les facteurs un par un.

2.3 Les puissances peuvent revenir à 1

Modulo 5, les puissances de 2 donnent 2, 4, 3, 1, puis recommencent. Fermat garantira un retour à 1 après $p-1$ étapes lorsque le module p est premier et ne divise pas la base. Il ne dira pas que cette période est la plus courte, ni que toute congruence réussie prouve la primalité.

Méthode | Une lecture active des preuves

Dans l'infinitude des premiers, repère où intervient la contradiction. Dans la factorisation, distingue existence et unicité. Dans Fermat, souligne les hypothèses avant de réduire l'exposant. Ces trois gestes correspondent à trois raisonnements différents.

3 Le cours formel

3.1 Nombres premiers et critère de recherche

Définition | Nombre premier

Un entier $p \geq 2$ est premier si ses seuls diviseurs positifs sont 1 et p. Un entier $n \geq 2$ qui n'est pas premier est composé. Les entiers 0 et 1 ne sont ni premiers ni composés.

2 est le seul nombre premier pair : un pair supérieur à 2 possède le diviseur 2 distinct de 1 et de lui-même. Être impair ne suffit pas : 9, 15 et 21 sont composés.

Théorème | Diviseur premier et borne de recherche

Tout entier $n \geq 2$ possède un diviseur premier. Si n est composé, il possède un diviseur premier inférieur ou égal à $\sqrt{n}$.

Démonstration | Justification des deux étapes

Pourquoi il existe un diviseur premier. Pour $n \geq 2$, la liste des diviseurs positifs de n supérieurs à 1 n'est pas vide, car elle contient n. Prenons son plus petit élément d. S'il n'était pas premier, il aurait un diviseur u avec $1 < u < d$. Écrire $d = uv$ et $n = dk$ donnerait $n = u(vk)$: u diviserait aussi n, tout en étant plus petit que d et supérieur à 1. Cela contredit le choix de d. Donc d est premier.
Pourquoi la racine carrée suffit pour un composé. Si n est composé, on peut écrire $n = ab$ avec $1 < a \leq b < n$, en rangeant les deux facteurs. Multiplier $a \leq b$ par $a > 0$ donne $a^2 \leq ab = n$, donc $a \leq \sqrt{n}$. Le premier résultat fournit un diviseur premier p de a. Comme $p \leq a$ et $a \mid n$, on a $p \mid n$ et $p \leq \sqrt{n}$.
Ainsi, si tous les premiers jusqu'à cette borne ont été testés sans succès, le nombre ne peut pas être composé. Il faut inclure la borne : pour $n = 49$, le facteur 7 est exactement sa racine carrée.

Méthode | Prouver la primalité d'un entier

Liste les nombres premiers inférieurs ou égaux à $\sqrt{n}$ et vérifie qu'aucun ne divise n. La borne est incluse : pour 49, il faut tester 7. Ne tester que quelques premiers sans atteindre cette borne ne conclut pas.

Exemple | Le nombre 97

Comme $9^2 = 81 < 97 < 100 = 10^2$, la racine carrée est entre 9 et 10. Les nombres premiers à tester jusqu'à cette borne sont exactement 2,3,5,7. Le nombre 97 est impair, donc non divisible par 2. Sa somme de chiffres est $9 + 7 = 16$, non divisible par 3. Son dernier chiffre n'est ni 0 ni 5, donc 5 ne le divise pas. Enfin $97 = 7 \times 13 + 6$, de reste non nul.
Tous les diviseurs premiers possibles d'un composé ont été exclus. Le critère de la racine carrée permet donc de conclure que 97 est premier. Tester 11 serait inutile, puisque 11 dépasse la borne.

À toi d'essayer : Une preuve de primalité doit finir les essais

101 est-il premier ? Explique pourquoi ton contrôle est complet.
Pour démarrer. Encadre la racine carrée pour savoir exactement quels premiers tester.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 26 Explication, p. 29

3.2 Il existe une infinité de nombres premiers

Théorème | Infinitude

L'ensemble des nombres premiers est infini.

Démonstration | Preuve d'Euclide

Hypothèse à contredire. Supposons qu'il n'existe qu'un nombre fini de premiers, réunis dans une liste complète $p_1, \ldots, p_k$. Nous construisons un entier qui oblige à sortir de cette liste.
Posons $P = p_1 \cdots p_k$ et $N = P + 1$. Comme $N \geq 2$, le résultat précédent lui garantit un diviseur premier q. Si la liste était complète, q serait l'un des p_j, donc diviserait leur produit P. Il divise aussi N par son choix. Un diviseur de deux entiers divise leur différence ; ainsi q diviserait $N - P = 1$. Or $q \geq 2$, donc il ne peut pas diviser 1 : contradiction.
Le premier q existe mais n'est pas dans la liste supposée complète. Cette impossibilité montre qu'aucune liste finie ne contient tous les nombres premiers. Nous n'avons pas supposé que N lui-même était premier : seule l'existence d'un facteur premier de N a servi.

Attention | Une conclusion plus précise que « le produit plus un est premier »

La preuve affirme que N possède un facteur premier nouveau, pas que N est lui-même premier. Par exemple $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$. La distinction évite une fausse généralisation.

Une preuve à construire : Un premier divise un produit

Si p est premier et $p \mid ab$, prouve que $p \mid a$ ou $p \mid b$.
Pour démarrer. Sépare les cas « p divise a » et « p ne divise pas a ».

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 26 Explication, p. 29

À toi d'essayer : Ce que prouve le produit plus un

À partir de la liste 2,3,5, calcule $N = 2 \times 3 \times 5 + 1$. Pourquoi un diviseur premier de N ne peut-il appartenir à cette liste ?
Pour démarrer. Compare N au produit 30 ; leur différence vaut 1.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 26 Explication, p. 29

3.3 Décomposition en facteurs premiers

Théorème | Existence et unicité

Tout entier $n \geq 2$ s'écrit comme produit de nombres premiers, de manière unique à l'ordre des facteurs près. En regroupant les facteurs identiques,

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \qquad \alpha_j \geq 1,$$

où les premiers p_j sont distincts.

Démonstration | Existence par récurrence forte

Initialisation. Le nombre 2 est premier : il est déjà un produit d'un seul facteur premier.
Hypothèse. Fixons $n \geq 3$ et supposons que *tous* les entiers $2, 3, \ldots, n-1$ possèdent une décomposition. Nous ne supposons pas seulement le résultat pour $n-1$, car les facteurs rencontrés peuvent être beaucoup plus petits.
Si n est premier, il fournit lui-même sa décomposition. Sinon, $n = ab$ avec $2 \leq a, b < n$. L'hypothèse s'applique à chacun : $a = p_1 \cdots p_r$ et $b = q_1 \cdots q_s$, où tous les facteurs sont premiers. Remplacer a, b dans $n = ab$ donne $n = p_1 \cdots p_r q_1 \cdots q_s$, une décomposition de n.
Les deux cas couvrent tous les entiers $n \geq 2$. La récurrence forte prouve donc l'existence pour chacun. À ce stade, elle ne prouve pas encore l'unicité ; celle-ci nécessite l'argument suivant.

Démonstration | Unicité avec Gauss

Supposons deux écritures $n = p_1 \cdots p_r = q_1 \cdots q_s$ en facteurs premiers. Puisque p_1 divise le premier produit, il divise aussi le second. Un premier qui divise un produit de deux facteurs divise l'un des deux ; en répétant cette propriété pour $q_1(q_2 \cdots q_s)$ puis pour les produits restants, on trouve un q_j divisible par p_1.
Mais q_j est premier. Ses seuls diviseurs positifs sont 1 et lui-même ; comme $p_1 \geq 2$, on a $p_1 = q_j$. Déplaçons ce facteur au début du second produit, ce que la commutativité autorise, puis divisons l'égalité par lui. Il reste une égalité entre les produits des facteurs restants.

Recommençons : chaque facteur du premier côté trouve un facteur identique de l'autre. Le nombre de facteurs diminue à chaque étape, donc le processus s'arrête. Si un côté n'avait plus de facteur alors que l'autre en avait encore, on aurait 1 égal à un produit de nombres tous au moins 2, impossible. Les deux listes ont donc la même longueur et les mêmes facteurs, avec les mêmes répétitions. Seul leur ordre peut différer.

Exemple | Factoriser 756

Divisons tant qu'un petit premier est possible : $756/2 = 378$, puis $378/2 = 189$. Le quotient 189 est impair, donc nous avons exactement deux facteurs 2. Sa somme de chiffres vaut 18, donc il est divisible par 3 : $189/3 = 63$, $63/3 = 21$, $21/3 = 7$. Nous avons trois facteurs 3, puis le facteur premier 7.
Ainsi $756 = 2\times2\times3\times3\times3\times7 = 2^2\times3^3\times7$. Tous les facteurs de base sont premiers. Le contrôle $4\times27\times7 = 108\times7 = 756$ vérifie les exposants. Une écriture contenant encore 21 ou 63 n'aurait pas terminé la décomposition en facteurs premiers.

À toi d'essayer : Une écriture vraiment première

Un élève propose $540 = 2^2\times3\times45$. Comment terminer et vérifier la décomposition ?
Pour démarrer. Décompose le facteur 45, puis additionne les exposants de la même base.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 26 Explication, p. 29

3.4 Lire les diviseurs, le PGCD et les carrés

Propriété | Exposants des diviseurs

Si $n = \prod p_j^{\alpha_j}$, les diviseurs positifs de n sont exactement les $d = \prod p_j^{\beta_j}$ avec $0 \le \beta_j \le \alpha_j$. Leur nombre vaut $\prod(\alpha_j+1)$. Un entier positif est un carré si et seulement si tous ses exposants premiers sont pairs.

Si $d \mid n$, on a $n = dq$ pour un entier positif q. Dans leurs factorisations premières, les exposants de d et de q s'additionnent pour donner ceux de n. Chaque exposant β_j de d est donc entre 0 et α_j ; aucun premier absent de n ne peut apparaître. Réciproquement, pour tout tel choix, le produit $q = \prod p_j^{\alpha_j-\beta_j}$ est un entier et $dq = n$, donc d est bien un diviseur.

Pour le premier exposant, on a α_1+1 choix en comptant zéro ; pour chacun, α_2+1 choix pour le deuxième, et ainsi de suite. L'unicité de la factorisation garantit que deux listes d'exposants différentes donnent deux diviseurs différents. D'où le produit des nombres de choix.

Si $n = m^2$ et $m = \prod p_j^{\gamma_j}$, alors $n = \prod p_j^{2\gamma_j}$: tous ses exposants sont pairs. Réciproquement, si $\alpha_j = 2\gamma_j$ pour chaque j, l'entier $m = \prod p_j^{\gamma_j}$ vérifie $m^2 = n$. Cela prouve les deux sens de la caractérisation des carrés. Le nombre 1 est aussi un carré, $1 = 1^2$, correspondant au produit vide.

Propriété | Comparer deux factorisations

Incluons tous les premiers apparaissant dans a ou b, avec exposant zéro s'ils sont absents de l'un. Pour qu'un nombre divise les deux, son exposant de chaque premier doit être au plus égal aux deux

exposants correspondants. Le plus grand choix possible est leur minimum. Le produit construit avec ces minima divise donc les deux nombres, et tout diviseur commun le divise : c'est le PGCD.
Pour être multiple des deux, chaque exposant doit au contraire être au moins égal à chacun des deux exposants. Leur maximum est le plus petit choix possible. Le produit de ces puissances est multiple des deux et divise tous leurs multiples communs : c'est le PPCM.
Pour deux exposants α, β, $\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta$. En multipliant PGCD et PPCM, l'exposant de chaque premier devient donc celui du produit ab. L'unicité de la factorisation donne $\gcd(a,b)\,\mathrm{ppcm}(a,b) = ab$.

Exemple | Deux descriptions complémentaires

Écrivons les mêmes premiers dans les deux nombres : $180 = 2^2\times3^2\times5^1\times7^0$ et $168 = 2^3\times3^1\times5^0\times7^1$.
Un diviseur commun ne peut utiliser que les exposants disponibles dans les deux, donc au plus les minima : $2^2 \times 3^1 = 12$. Un multiple commun doit contenir assez de facteurs pour les deux, donc au moins les maxima : $2^3 \times 3^2 \times 5 \times 7 = 2520$.
Pour un diviseur de 180, l'exposant de 2 peut être 0,1,2 (trois choix), celui de 3 aussi (trois choix), celui de 5 peut être 0 ou 1 (deux choix). Chaque triplet donne un diviseur distinct par unicité de la factorisation, donc il y en a $3 \times 3 \times 2 = 18$. L'exposant zéro signifie qu'on n'utilise pas ce facteur, ce qui inclut le diviseur 1.

À toi d'essayer : Compter sans oublier le diviseur 1

Combien 72 possède-t-il de diviseurs positifs ? Combien sont des carrés ?
Pour démarrer. Liste les exposants autorisés, puis garde seulement les exposants pairs pour les carrés.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 27 Explication, p. 30

3.5 Petit théorème de Fermat : deux versions

Théorème | Fermat

Si p est premier et a un entier non divisible par p, alors $a^{p-1} \equiv 1 \pmod p$. Pour tout entier a, sans condition supplémentaire, $a^p \equiv a \pmod p$.

Démonstration | Passer d'une version à l'autre

Supposons d'abord la version $a^{p-1} \equiv 1$ pour $p \nmid a$. Multiplier ses deux membres par a donne $a^p \equiv a$. Si au contraire $p \mid a$, alors $a \equiv 0$, et sa puissance a^p est aussi congrue à 0 : la seconde version est encore vraie. Les deux cas couvrent tous les entiers a.
Pour revenir de $a^p \equiv a$ à la première version, nous devons supposer $p \nmid a$. Comme p est premier, cela implique $\gcd(a,p) = 1$, donc a possède un inverse u modulo p. Multiplier par u donne $ua^p \equiv ua$, soit $a^{p-1} \equiv 1$. C'est cet inverse qui justifie la simplification ; pour une base divisible par p, il n'existe pas et la simplification serait fausse.

Démonstration | Preuve par permutation des restes, prolongement

But. Nous allons multiplier les restes de $a, 2a, \dots, (p-1)a$ et montrer qu'ils sont simplement les nombres $1, \dots, p-1$ rangés autrement.
Comme p est premier et ne divise pas a, $\gcd(p, a) = 1$. Aucun ak avec $1 \leq k \leq p-1$ n'est divisible par p : sinon Gauss donnerait $p \mid k$, impossible entre 1 et $p-1$. Les restes sont donc tous dans $\{1, \dots, p-1\}$.
Si deux restes étaient égaux, $ak \equiv a\ell$, donc $p \mid a(k-\ell)$. Gauss donnerait $p \mid (k-\ell)$. Or $-(p-1) < k - \ell < p-1$, donc le seul multiple possible est 0 : $k = \ell$. Les $p-1$ restes sont distincts dans un ensemble de $p-1$ valeurs ; ils occupent donc toutes les places, une fois chacune.
Multiplions les congruences correspondantes. Le produit gauche est $a \times 2a \times \cdots \times (p-1)a = a^{p-1}(1 \times 2 \times \cdots \times (p-1))$. Le produit droit est $(p-1)!$, la factorielle. Ainsi $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$.
Aucun des facteurs $1, \dots, p-1$ n'est divisible par p. La propriété du premier divisant un produit montre donc que p ne divise pas leur produit. Il est premier avec $(p-1)!$, qui possède un inverse modulo p. Multiplier par cet inverse donne $a^{p-1} \equiv 1$. La simplification finale est ainsi justifiée, et non supposée.

Méthode | Réduire un exposant

Vérifie que le module p est premier et que p ne divise pas a. Écris l'exposant $N = (p-1)q + r$. Alors $a^N \equiv a^r \pmod{p}$. Chercher un cycle plus court peut encore accélérer le calcul.

Exemple | Une grande puissance

Le module 7 est premier et ne divise pas la base 3. Fermat s'applique donc : $3^{7-1} = 3^6 \equiv 1 \pmod{7}$. Divisons l'exposant par 6 : $100 = 6 \times 16 + 4$. Alors $3^{100} = (3^6)^{16} 3^4 \equiv 1^{16} 3^4 = 81 \equiv 4 \pmod{7}$, car $81 = 7 \times 11 + 4$.
Le reste final 4 appartient à $\{0, \dots, 6\}$. Réduire 100 modulo 7 serait injustifié : Fermat fournit une puissance d'exposant $p - 1 = 6$, et c'est par cet exposant que l'on regroupe les facteurs.

Attention | Fermat ne donne pas une réciproque

Si $a^{n-1} \not\equiv 1 \pmod{n}$ avec $\gcd(a, n) = 1$, alors n n'est pas premier : a est un témoin. Si l'égalité est vérifiée, cela ne prouve pas la primalité. Par exemple $341 = 11 \times 31$ et $2^{10} = 1024 \equiv 1 \pmod{341}$, donc $2^{340} \equiv 1$, bien que 341 soit composé.

À toi d'essayer : Vérifier les hypothèses

Peut-on affirmer $6^{10} \equiv 1 \pmod{11}$? Et $11^{10} \equiv 1 \pmod{11}$?
Pour démarrer. Vérifie séparément la primalité du module et la non-divisibilité de la base.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 27 Explication, p. 30

À toi d'essayer : Réduire le bon exposant

Calcule le reste de 2^{100} modulo 11 en explicitant les hypothèses.
Pour démarrer. Applique Fermat avec $p = 11$, puis regroupe l'exposant en paquets de $p - 1$.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 27 Explication, p. 30

3.6 Trois algorithmes exacts

3.6.1 Crible d'Ératosthène

Pour lister les premiers jusqu'à N, marque tous les entiers de 2 à N comme candidats. À chaque premier p encore marqué, supprime ses multiples à partir de p^2 ; les multiples plus petits ont déjà un facteur premier inférieur à p.

```
def crible(N):
    if N < 2:
        return []
    premier = [True] * (N + 1)
    premier[0] = premier[1] = False
    p = 2
    while p*p <= N:
        if premier[p]:
            for k in range(p*p, N + 1, p):
                premier[k] = False
        p += 1
    return [k for k in range(2, N + 1) if premier[k]]
```

Le critère du diviseur inférieur ou égal à la racine carrée garantit qu'à l'arrêt aucun entier composé ne reste marqué.

3.6.2 Décomposition

```
def facteurs(n):
    if n < 2:
        raise ValueError("n >= 2 requis")
    resultat = []
    d = 2
    while d*d <= n:
        while n % d == 0:
            resultat.append(d)
            n //= d
        d += 1
    if n > 1:
        resultat.append(n)
    return resultat
```

Le produit des facteurs déjà extraits et de n courant reste égal au nombre initial. Après les divisions par les petits facteurs, le n final, s'il est supérieur à 1, est premier ; sinon il aurait encore un diviseur au plus égal à sa racine carrée.

3.6.3 Exponentiation rapide modulaire

```python
def puissance_rapide(a, N, m):
    if N < 0 or m < 1:
        raise ValueError("N >= 0 et m >= 1 requis")
    r, b, e = 1 % m, a % m, N
    while e > 0:
        if e % 2 == 1:
            r = (r*b) % m
        b = (b*b) % m
        e //= 2
    return r
```

Pourquoi ce code calcule la bonne puissance. Les variables sont un résultat partiel r, une base courante b et un exposant restant e. Au départ $r = 1 \bmod m$, $b = a \bmod m$, $e = N$, donc $rb^e \equiv a^N$.

Si $e = 2k$ est pair, $rb^e = r(b^2)^k$. Mettre la base au carré et diviser l'exposant par deux conserve donc le produit représenté. Si $e = 2k + 1$ est impair, $rb^e = (rb)(b^2)^k$: il faut d'abord transférer un facteur b dans r, puis faire les mêmes changements. C'est exactement la branche `if`, suivie des deux affectations. Les réductions modulo m conservent la congruence et évitent de stocker de trop grands entiers.

À chaque tour avec $e > 0$, la division entière par 2 donne un entier plus petit, donc la boucle s'arrête à $e = 0$. L'invariant devient alors $r \equiv a^N$ car $b^0 = 1$. Comme r est entre 0 et $m - 1$, c'est le reste recherché. Pour $N = 0$, aucun tour n'est nécessaire ; le reste de 1 est déjà correct. Pour $m = 1$, il vaut 0. Diviser l'exposant par deux à chaque tour explique pourquoi quelques tours suffisent même pour un grand exposant.

À toi d'essayer : Suivre l'exponentiation rapide

Pour calculer 3^{13} modulo 7, pars de $(r, b, e) = (1, 3, 13)$. Donne le triplet après le premier tour et vérifie l'invariant.
Pour démarrer. Traite d'abord l'exposant impair, puis calcule les deux autres affectations.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 27 Explication, p. 30

4 Boîte à outils — factoriser ou réduire ?

4.1 Deux premières questions qui évitent des calculs inutiles

Cherches-tu à prouver qu'un nombre est premier, ou à calculer un reste ? Dans le premier cas, un test de diviseurs peut être concluant ; dans le second, une factorisation complète du nombre étudié est souvent superflue. Le petit théorème de Fermat réduit les puissances lorsque le module est premier, tandis que la division euclidienne garde les calculs de petite taille.

Exemple | Calculer modulo un composé à l'aide de deux premiers

Pour calculer 2^{100} modulo 35, on ne peut pas appliquer directement Fermat au module 35, qui est composé. Travaillons avec $35 = 5 \times 7$.

Modulo 5, Fermat donne $2^4 \equiv 1$, donc $2^{100} = (2^4)^{25} \equiv 1$. Modulo 7, il donne $2^6 \equiv 1$. Comme $100 = 6 \times 16 + 4$, on obtient $2^{100} \equiv 2^4 = 16 \equiv 2 \pmod 7$. Les deux applications sont légitimes : 5 et 7 sont premiers et ne divisent pas 2.
Le reste r modulo 35 doit être entre 0 et 34 et congru à 1 modulo 5. Les possibilités sont $1, 6, 11, 16, 21, 26, 31$. Leurs restes modulo 7 sont respectivement $1, 6, 4, 2, 0, 5, 3$. Seul 16 a le reste 2 voulu.
Justifions que ces deux informations suffisent : $D = 2^{100} - 16$ est divisible par 5 et par 7. Écrivons $D = 5k$. Comme $7 \mid 5k$ et $\gcd(7, 5) = 1$, Gauss donne $7 \mid k$, donc $35 \mid D$. Le nombre 16 appartient bien à l'intervalle des restes : c'est donc le reste recherché.

4.2 Diviseurs soumis à une condition

Pour $n = 2^4 \times 3^2 \times 5$, tout diviseur positif s'écrit $2^a 3^b 5^c$, avec $0 \leq a \leq 4$, $0 \leq b \leq 2$, $0 \leq c \leq 1$. Il y a 5×3×2=30 diviseurs en tout. Un diviseur impair impose a=0 : il en reste 3×2=6. Un diviseur carré impose a pair, b pair et c=0 : les choix sont a dans 0,2,4, b dans 0,2, donc six diviseurs carrés. Le calcul se construit à partir des exposants autorisés, pas à partir d'une nouvelle formule à mémoriser.

4.3 Pourquoi les candidats non premiers du code ne gênent pas

L'algorithme de factorisation essaie d=2,3,4,5,..., sans calculer d'avance la liste des premiers. Si d est composé, ses facteurs premiers plus petits ont déjà été totalement retirés du reste n ; il ne peut donc plus le diviser. Ce passage supplémentaire ralentit un peu l'algorithme, mais ne change pas sa correction. Si le reste devient 1, la factorisation est terminée ; si d^2 le dépasse, le reste éventuellement supérieur à 1 est premier.

Exemple | Suivre l'invariant sur 84

Au départ, aucun facteur n'est extrait et le nombre courant vaut 84. La première division par 2 extrait un facteur et laisse 42 : $2 \times 42 = 84$. La deuxième laisse 21 : $2 \times 2 \times 21 = 84$. Une troisième division par 2 est impossible car 21 est impair. Avec 3, on extrait un facteur et laisse 7 : $2 \times 2 \times 3 \times 7 = 84$.
Le produit des facteurs extraits multiplié par le nombre courant reste donc toujours 84 : c'est l'invariant. Le facteur restant 7 est premier ; la liste finale est $[2, 2, 3, 7]$. La répétition de 2 dans la liste correspond à l'exposant 2 de la factorisation $2^2 \times 3 \times 7$, pas à deux facteurs différents.

À toi d'essayer : Décrire des diviseurs carrés

Quels sont les diviseurs positifs de 72 qui sont des carrés ?
Pour démarrer. Un carré exige un nombre pair de répétitions de chaque facteur premier.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 28 Explication, p. 30

À toi d'essayer : Réfuter un mauvais usage de Fermat

Un élève affirme que $2^8 \equiv 1 \pmod 9$ parce que 2 n'est pas divisible par 9. Vérifie.
Pour démarrer. Avant le calcul, identifie quelle hypothèse de Fermat manque.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 28 Explication, p. 31

5 Exercices progressifs

Les exercices 1 à 5 consolident les bases, 6 à 10 relient les notions et 11 à 15 demandent davantage d'initiative. Cherche d'abord, puis utilise un indice si tu en as besoin.

Exercice 1 — Définition précise ★☆☆

Parmi 1, 2, 21, 29 et 49, lesquels sont premiers ? Justifie.

Exercice 2 — Factorisation ★☆☆

Décompose 360 et 504 en facteurs premiers.

Exercice 3 — Nombre de diviseurs ★☆☆

Combien 360 possède-t-il de diviseurs positifs ?

Exercice 4 — PGCD par facteurs ★☆☆

Calcule le PGCD et le PPCM de 360 et 504.

Exercice 5 — Fermat direct ★☆☆

Calcule le reste de 2^{30} modulo 7.

Exercice 6 — Primalité de 127 ★★☆

Prouve que 127 est premier.

Exercice 7 — Compléter un carré ★★☆

Trouve le plus petit entier positif k tel que $756k$ soit un carré.

Exercice 8 — Grande puissance ★★☆

Calcule 5^{2026} modulo 13.

Exercice 9 — Un inverse avec Fermat ★★☆

Utilise Fermat pour exprimer un inverse de 3 modulo 7 et donne son représentant entre 0 et 6.

Exercice 10 — Une réciproque fausse ★★☆

Vérifie que 341 est composé mais que $2^{340} \equiv 1 \pmod{341}$.

Exercice 11 — Un témoin de composition ★★★

Calcule 2^{14} modulo 15. Que peut-on en déduire sans factoriser 15 ?

Exercice 12 — Un exposant nécessaire ★★★

Pour $n \geq 2$, montre que si $2^n - 1$ est premier, alors n est premier. La réciproque est-elle vraie ?

Exercice 13 — Crible ★★★

Exécute le crible jusqu'à 30. Pourquoi peut-on s'arrêter après le passage de 5 ?

Exercice 14 — Puissance rapide ⭐⭐⭐

Calcule $7^{13} \pmod{11}$ par carrés successifs, puis compare à Fermat.

Exercice 15 — Un argument d'irrationalité ⭐⭐⭐

Prouve que $\sqrt{6}$ est irrationnel en utilisant l'unicité de la factorisation.

6 🚀 Problème — Pour aller plus loin

Ce prolongement est accessible à partir du cours : les résultats supplémentaires sont guidés, et leur mémorisation n'est pas un préalable. Tu peux répartir la recherche sur plusieurs séances.

Un modèle RSA entièrement démontré

On choisit $p = 5$, $q = 11$, $N = pq = 55$ et $e = 3$. Un message est un entier $m \in \{0, \dots, 54\}$; son chiffré c est le reste de m^3 modulo 55. Ce petit modèle sert au calcul : ces nombres sont trop petits pour une utilisation réelle. Durée indicative : 90 minutes.

Partie I — Construire l'exposant inverse

1. Calcule $(p-1)(q-1)$ et vérifie $\gcd(3, 40) = 1$.
2. Trouve d entre 1 et 39 tel que $3d \equiv 1 \pmod{40}$.
3. Chiffre $m = 7$. Montre que déchiffrer par c^d revient à calculer m^{81} modulo 55.

Partie II — Une preuve valable pour tous les messages

1. Si 5 ne divise pas m, utilise Fermat pour montrer $m^{81} \equiv m \pmod{5}$. Traite séparément le cas $5 \mid m$.
2. Fais de même modulo 11.
3. En utilisant Gauss, conclus $m^{81} \equiv m \pmod{55}$. Pourquoi fallait-il traiter aussi les multiples de 5 ou de 11 ?

Partie III — Mettre en œuvre

1. Déchiffre le résultat de la partie I par carrés successifs.
2. Chiffre puis déchiffre $m = 5$ en expliquant pourquoi la preuve reste valable.
3. Écris deux fonctions Python sur les entiers, et une vérification pour les 55 messages possibles.

Pistes

$3 \times 27 = 81 = 1 + 2 \times 40$. Pour chaque premier, distingue une base nulle d'une base inversible. Une différence divisible par 5 et 11 est divisible par 55.

7 Indices des exercices

Exercice 1

Un contre-exemple de diviseur suffit pour montrer qu'un nombre est composé.

Pour prouver la primalité, couvre tous les premiers jusqu'à la racine.

Exercice 2

Extrais d'abord les facteurs 2.

Poursuis avec 3 puis le facteur restant.

Exercice 3

Chaque exposant peut aller de zéro à celui de 360.

N'oublie pas le choix zéro.

Exercice 4

Aligne les mêmes premiers dans les deux décompositions.

Un premier absent a pour exposant zéro.

Exercice 5

Vérifie le module et la base.

30 est un multiple de 6.

Exercice 6

La borne de recherche est entre 11 et 12.

Le test de 11 ne doit pas être oublié.

Exercice 7

Repère les exposants impairs.

Ajoute exactement un facteur de chaque premier concerné.

Exercice 8

Fermat réduit l'exposant modulo 12.

Cherche ensuite une petite puissance particulièrement simple.

Exercice 9

Isole un facteur 3 dans la puissance sixième.

Réduis le résultat pour obtenir un petit représentant.

Exercice 10

Factorise 341.

Une petite puissance suffit à justifier la grande.

Exercice 11

Cherche le cycle modulo 15.

Applique la contraposée de Fermat.

Exercice 12

Factorise une différence de puissances.

Prouve que les deux facteurs sont non triviaux.

Exercice 13

Marque les multiples à partir du carré du premier.

Utilise le critère de la racine carrée pour justifier l'arrêt.

Exercice 14

Écris 13 comme somme de puissances de 2.

Réduis chaque carré immédiatement.

Exercice 15

Compare un seul exposant premier des deux côtés.

Les exposants d'un carré sont tous pairs.

8 Corrigés détaillés

Corrigé 1

Démonstration / Solution expliquée

1 ne remplit pas la condition $p \geq 2$ de la définition. 2 a exactement les diviseurs positifs 1 et 2, donc est premier. Le nombre 21 est composé puisque $21 = 3 \times 7$, avec deux facteurs supérieurs à 1. De même $49 = 7^2$ est composé.
Pour 29, $5^2 < 29 < 6^2$, donc les seuls premiers à tester sont 2,3,5. Il est impair ; sa somme de chiffres 11 n'est pas divisible par 3 ; son dernier chiffre n'est ni 0 ni 5. Aucun candidat ne le divise, donc 29 est premier. Les nombres premiers de la liste sont exactement 2 et 29.

Corrigé 2

Démonstration / Solution expliquée

Pour 360, les divisions par 2 donnent $360 \to 180 \to 90 \to 45$, soit trois facteurs 2. Puis $45 \to 15 \to 5$ par divisions par 3, soit deux facteurs 3, et le dernier facteur est 5. Donc $360 = 2^3 \times 3^2 \times 5$; contrôle $8 \times 9 \times 5 = 360$.
Pour 504, les divisions par 2 donnent $504 \to 252 \to 126 \to 63$, puis celles par 3 donnent $63 \to 21 \to 7$. Ainsi $504 = 2^3 \times 3^2 \times 7$; contrôle $8 \times 9 \times 7 = 504$. Tous les facteurs de base 2,3,5,7 sont premiers.

Corrigé 3

Démonstration / Solution expliquée

La décomposition est $360 = 2^3 \times 3^2 \times 5^1$. Un diviseur positif s'écrit $2^a 3^b 5^c$, avec $a \in \{0,1,2,3\}$, $b \in \{0,1,2\}$ et $c \in \{0,1\}$. Il y a quatre choix pour a ; pour chacun, trois choix pour b ; pour chacune de ces paires, deux choix pour c. Cela fait $4 \times 3 \times 2 = 24$ diviseurs.
L'unicité de la factorisation garantit que deux triplets différents ne donnent pas le même diviseur. Le triplet $(0,0,0)$ donne 1 ; oublier les exposants nuls ferait manquer des diviseurs.

Corrigé 4

Démonstration / Solution expliquée

Les factorisations sont $360 = 2^3 3^2 5^1 7^0$ et $504 = 2^3 3^2 5^0 7^1$. Pour diviser les deux, on prend les exposants minimaux : le PGCD est $2^3 3^2 = 72$. Pour être multiple des deux, on prend les maximaux : le PPCM est $2^3 3^2 5 \times 7 = 2520$.
Les facteurs 5 et 7 n'entrent pas dans le PGCD, car chacun manque dans l'un des nombres. Ils entrent tous deux dans le PPCM. Contrôle : $72 \times 2520 = 181440$ et $360 \times 504 = 181440$, comme l'identité PGCD fois PPCM le prévoit.

Corrigé 5

Démonstration / Solution expliquée

Le module 7 est premier et la base 2 n'est pas divisible par 7. Les deux hypothèses de Fermat sont donc vérifiées. Il donne $2^6 \equiv 1 \pmod 7$.
Comme $30 = 6 \times 5$, $2^{30} = (2^6)^5 \equiv 1^5 = 1$. Le nombre 1 est un reste autorisé entre 0 et 6, donc c'est le reste demandé. On peut contrôler avec le cycle plus court $2^3 = 8 \equiv 1$: $30 = 3 \times 10$ donne le même résultat.

Corrigé 6

Démonstration / Solution expliquée

$11^2 = 121 < 127 < 144 = 12^2$, donc il faut tester tous les premiers jusqu'à 11 : 2,3,5,7,11. Le nombre est impair ; sa somme de chiffres vaut $1+2+7 = 10$, non divisible par 3 ; son dernier chiffre n'est ni 0 ni 5. Pour les deux autres, $127 = 7 \times 18 + 1$ et $127 = 11 \times 11 + 6$.
Aucun de ces cinq premiers ne le divise. Un composé aurait obligatoirement un diviseur premier au plus égal à sa racine carrée ; cette possibilité est entièrement exclue. Donc 127 est premier. Oublier 11 aurait laissé le raisonnement incomplet.

Corrigé 7

Démonstration / Solution expliquée

$756 = 2^2 \times 3^3 \times 7^1$. Pour que le produit par k soit un carré, chaque exposant total doit être pair. L'exposant de 2 est déjà pair ; celui de 3 manque d'un facteur 3 pour devenir 4 ; celui de 7 manque d'un facteur 7 pour devenir 2. Le plus petit choix est donc $k = 3 \times 7 = 21$.
Le produit est $2^2 \times 3^4 \times 7^2 = (2 \times 3^2 \times 7)^2 = 126^2$. Pour justifier la minimalité, toute solution doit apporter un exposant impair positif de 3 et de 7, donc au moins un facteur de chacun ; tous les autres exposants ajoutés sont pairs. Ainsi tout k admissible s'écrit $21s^2$ avec $s \geq 1$ entier. Le minimum correspond à $s = 1$.

Corrigé 8

Démonstration / Solution expliquée

Le module 13 est premier et ne divise pas 5, donc $5^{12} \equiv 1 \pmod{13}$. La division $2026 = 12 \times 168 + 10$ donne $5^{2026} \equiv 5^{10}$.
Pour calculer cette dernière puissance, $5^2 = 25 = 2 \times 13 - 1$, donc $5^2 \equiv -1$. Alors $5^{10} = (5^2)^5 \equiv (-1)^5 = -1$. Le reste euclidien doit être positif ou nul : $-1 \equiv 12 \pmod{13}$. Le reste demandé est donc 12. Le représentant négatif a simplifié le calcul, mais la réponse finale est dans $\{0, \ldots, 12\}$.

Corrigé 9

Démonstration / Solution expliquée

Comme 7 est premier et ne divise pas 3, Fermat donne $3^6 \equiv 1 \pmod 7$. En écrivant $3^6 = 3 \times 3^5$, on voit que 3^5 est un inverse de 3 modulo 7.
Le nombre $3^5 = 243$ a pour division $243 = 7 \times 34 + 5$. Son représentant entre 0 et 6 est donc 5. Vérification directe : $3 \times 5 = 15 = 2 \times 7 + 1$. L'exposant $p - 2 = 5$ est choisi parce qu'un facteur 3 est déjà placé devant la puissance pour former l'exposant $p - 1 = 6$.

Corrigé 10

Démonstration / Solution expliquée

$11 \times 31 = 341$ avec deux facteurs strictement supérieurs à 1, donc 341 est composé. Pourtant $2^{10} = 1024 = 3 \times 341 + 1$, donc $2^{10} \equiv 1 \pmod{341}$. Élever cette congruence à la puissance 34 donne $2^{340} = (2^{10})^{34} \equiv 1$.
Le nombre passe donc la congruence que Fermat imposerait à un premier pour la base 2, mais il n'est pas premier. Cela réfute la réciproque « si cette congruence est vraie, le module est premier ». Une condition nécessaire n'est pas automatiquement suffisante.

Corrigé 11

Démonstration / Solution expliquée

$2^4 = 16 \equiv 1 \pmod{15}$. Puisque $14 = 4 \times 3 + 2$, $2^{14} = (2^4)^3 2^2 \equiv 1^3 \times 4 = 4$, et non 1.
Si 15 était premier, il ne diviserait pas 2, et Fermat exigerait $2^{15-1} \equiv 1 \pmod{15}$. Le calcul contredit cette conséquence. Donc 15 n'est pas premier. Comme il est supérieur à 1, il est composé. Ce raisonnement utilise la contraposée de Fermat et ne nécessite pas de trouver ses facteurs.

Corrigé 12

Démonstration / Solution expliquée

Prouvons la contraposée : supposons n composé, donc $n = ab$ avec $a, b \geq 2$. Posons $u = 2^a$. L'identité $u^b - 1 = (u-1)(1 + u + \cdots + u^{b-1})$ donne

$$2^n - 1 = (2^a - 1)(1 + 2^a + \cdots + 2^{a(b-1)}).$$

Le premier facteur est au moins $2^2 - 1 = 3$; le second contient au moins $1 + 2^a \geq 5$. Les deux sont supérieurs à 1, donc $2^n - 1$ est composé. Par contraposée, sa primalité impose celle de n.
La réciproque est fausse : 11 est premier, mais $2^{11} - 1 = 2047 = 23 \times 89$. Les deux facteurs sont non triviaux, ce qui suffit à prouver que 2047 est composé.

Corrigé 13

Démonstration | Solution expliquée

On conserve d'abord les candidats de 2 à 30. Le passage de 2 barre $4, 6, 8, \ldots, 30$. Celui de 3 commence à 9 et barre $9, 12, 15, 18, 21, 24, 27, 30$; certains étaient déjà barrés. Celui de 5 commence à 25 et barre 25 et 30. Les candidats restants sont $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.
Pourquoi s'arrêter ? $\sqrt{30} < 6$, donc tout composé de cette liste initiale aurait un diviseur premier parmi 2,3,5. Tous leurs multiples composés ont été barrés. Aucun autre passage ne peut découvrir un composé oublié ; les nombres restants sont donc exactement les premiers jusqu'à 30.

Corrigé 14

Démonstration | Solution expliquée

Réduisons chaque carré modulo 11 : $7^2 = 49 \equiv 5$; $7^4 \equiv 5^2 = 25 \equiv 3$; $7^8 \equiv 3^2 = 9$. Puis $13 = 8 + 4 + 1$, donc $7^{13} = 7^8 7^4 7 \equiv 9 \times 3 \times 7$. Le produit vaut 189, et $189 = 17 \times 11 + 2$, donc le reste est 2.
Fermat donne un contrôle : 11 est premier et ne divise pas 7, donc $7^{10} \equiv 1$. Ainsi $7^{13} \equiv 7^3 \equiv 5 \times 7 = 35 \equiv 2$. Les deux méthodes concordent ; les carrés successifs auraient aussi fonctionné avec un module composé.

Corrigé 15

Démonstration | Solution expliquée

Supposons au contraire $\sqrt{6} = p/q$ avec p, q entiers positifs. En élevant au carré puis en multipliant par q^2, on obtient $p^2 = 6q^2$.
Notons α l'exposant de 2 dans p et β celui de 2 dans q ; ils peuvent valoir zéro. Dans p^2, l'exposant est 2α, pair. Dans $6q^2 = 2 \times 3 \times q^2$, il est $1 + 2\beta$, impair. L'égalité des deux entiers imposerait l'égalité de ces exposants par unicité de la factorisation, donc $2\alpha = 1 + 2\beta$, impossible. L'hypothèse rationnelle est contradictoire ; $\sqrt{6}$ est irrationnel.

9 Corrigé du problème

Partie I — Construire une opération inverse

1. $(p-1)(q-1) = (5-1)(11-1) = 4 \times 10 = 40$. La division $40 = 13 \times 3 + 1$ donne un reste 1, donc $\gcd(3, 40) = 1$: un inverse de 3 existe modulo 40.

2. L'identité $1 = 40 - 13 \times 3$ donne l'inverse -13. Son représentant positif est $-13 + 40 = 27$. Il est bien entre 1 et 39 et $3 \times 27 = 81 = 2 \times 40 + 1$. On choisit donc $d = 27$.

3. Pour $m = 7$, $m^3 = 343 = 6 \times 55 + 13$, donc le code chiffré est $c = 13$. Comme $c \equiv m^3 \pmod{55}$, élever à la puissance 27 conserve la congruence : $c^{27} \equiv (m^3)^{27} = m^{81}$. Il reste à prouver que cette dernière puissance retrouve m.

Partie II — Couvrir aussi les bases non inversibles

1. Si 5 ne divise pas m, Fermat donne $m^4 \equiv 1 \pmod 5$. Écrivons $81 = 1 + 4 \times 20$: $m^{81} = m(m^4)^{20} \equiv m \times 1 = m$. Si 5 divise m, les deux membres m^{81} et m sont divisibles par 5, donc encore congrus. Les deux cas couvrent tous les messages modulo 5.

2. Si 11 ne divise pas m, Fermat donne $m^{10} \equiv 1 \pmod{11}$. Comme $81 = 1 + 10 \times 8$, $m^{81} = m(m^{10})^8 \equiv m$. Si 11 divise m, les deux membres sont congrus à zéro. La conclusion vaut donc aussi pour tous les messages modulo 11.

3. La différence $D = m^{81} - m$ est divisible par 5 et 11. Écrivons $D = 5k$. Comme $11 \mid 5k$ et $\gcd(11, 5) = 1$, Gauss donne $k = 11\ell$. Ainsi $D = 55\ell$, donc $m^{81} \equiv m \pmod{55}$. Le déchiffrement renvoie un reste entre 0 et 54, tout comme le message initial ; deux représentants congrus dans cet intervalle sont égaux. Il retrouve donc exactement m. Omettre les cas divisibles par 5 ou 11 aurait laissé par exemple $m = 5$ sans preuve.

Partie III — Calculer et vérifier

1. Pour $c = 13$, les carrés successifs modulo 55 sont : $13^2 = 169 \equiv 4$; $13^4 \equiv 4^2 = 16$; $13^8 \equiv 16^2 = 256 \equiv 36$; $13^{16} \equiv 36^2 = 1296 \equiv 31$. Les restes se vérifient par $169 = 3 \times 55 + 4$, $256 = 4 \times 55 + 36$, $1296 = 23 \times 55 + 31$.

Comme $27 = 16 + 8 + 2 + 1$, $13^{27} \equiv 31 \times 36 \times 4 \times 13$. Réduisons progressivement : $31 \times 36 = 1116 \equiv 16$; $16 \times 4 = 64 \equiv 9$; $9 \times 13 = 117 \equiv 7$. On retrouve le message 7.

2. Pour $m = 5$, le chiffré est $5^3 = 125 = 2 \times 55 + 15$, donc $c = 15$. Les carrés donnent $15^2 = 225 \equiv 5$, $15^4 \equiv 25$, $15^8 \equiv 625 \equiv 20$, $15^{16} \equiv 400 \equiv 15$. Alors $15^{27} \equiv 15 \times 20 \times 5 \times 15$. Les produits réduits valent successivement $300 \equiv 25$, $125 \equiv 15$, $225 \equiv 5$. Le message 5 est bien retrouvé. Il est non inversible modulo 55, mais la preuve de la partie II traitait explicitement ce cas.

3. Python calcule ces puissances exactement avec trois arguments dans `pow` : la base, l'exposant et le module.

```python
def chiffrer(m):
    return pow(m, 3, 55)

def dechiffrer(c):
    return pow(c, 27, 55)

assert all(dechiffrer(chiffrer(m)) == m for m in range(55))
```

`range(55)` fournit tous les messages de 0 à 54. Pour chacun, on chiffre puis déchiffre et on compare au message initial. `all` exige que les 55 comparaisons soient vraies ; `assert` signale une erreur si ce n'est pas le cas. Ce contrôle exhaustif vérifie ces valeurs, tandis que la partie II explique mathématiquement le fonctionnement et le traitement des cas non inversibles.

10 Faire le point par une variante autonome

Essaie cette variante sans relire le corrigé précédent. Explique le choix de ta méthode, puis utilise les contrôles pour décider quelle notion retravailler.

À toi d'essayer : Fermat et factorisation dans le même calcul

Calcule le reste de 2^{20} modulo 15 en étudiant séparément les modules 3 et 5.
Pour démarrer. Prouve deux divisibilités pour $2^{20}-1$, puis réunis-les avec Gauss.

Tu peux chercher, prendre un indice ou lire l'explication, à ton rythme.

Indices, p. 28 Explication, p. 31

11 Fiche-mémoire

— Premier : entier au moins 2 ayant exactement deux diviseurs positifs.
— Un composé a un diviseur premier au plus égal à sa racine carrée.
— Un premier divisant un produit divise au moins un facteur ; les facteurs premiers d'un entier sont uniques à l'ordre près.
— Fermat : $a^{p-1} \equiv 1 \pmod{p}$ si p est premier et $p \nmid a$; $a^p \equiv a$ pour tout entier a.
— Fermat peut réfuter une primalité ; une congruence réussie pour une base ne la prouve pas.
— Crible, divisions successives et carrés successifs répondent à trois questions différentes : lister, factoriser, calculer une puissance.

Contrôle. Ai-je inclus la borne racine carrée ? Vérifié les hypothèses de Fermat ? Réduit l'exposant modulo p-1 ? Évité de confondre un nombre et un diviseur premier de ce nombre ?

12 Indices des pauses et des preuves

Chercher avec un indice fait partie du travail. Tu peux revenir à l'énoncé avec le lien sous chaque aide.

Une preuve de primalité doit finir les essais

Indice 1 — Une piste.

Sa racine carrée est entre 10 et 11.

Indice 2 — Un pas de plus.

Les candidats premiers sont 2,3,5 et 7.

Revenir à la recherche, p. 5

Un premier divise un produit

Indice 1 — Une piste.

Si p ne divise pas a, que vaut leur PGCD ?

Indice 2 — Un pas de plus.

Les seuls diviseurs positifs de p sont 1 et p.

Revenir à la recherche, p. 6

Ce que prouve le produit plus un

Indice 1 — Une piste.

N vaut 31, mais raisonne avec la différence de deux multiples.

Indice 2 — Un pas de plus.

Un diviseur commun du produit et du produit plus un diviserait 1.

Revenir à la recherche, p. 6

Une écriture vraiment première

Indice 1 — Une piste.

Le facteur 45 n'est pas premier.

Indice 2 — Un pas de plus.

$45 = 3^2 \times 5$.

Revenir à la recherche, p. 7

Compter sans oublier le diviseur 1

Indice 1 — Une piste.

$72 = 2^3 \times 3^2$.

Indice 2 — Un pas de plus.

Un diviseur choisit un exposant pour 2 et pour 3 ; un carré exige des exposants pairs.

Revenir à la recherche, p. 8

Vérifier les hypothèses

Indice 1 — Une piste.

Le module 11 est premier dans les deux cas.

Indice 2 — Un pas de plus.

La base doit aussi être non divisible par 11.

Revenir à la recherche, p. 10

Réduire le bon exposant

Indice 1 — Une piste.

11 est premier et ne divise pas 2.

Indice 2 — Un pas de plus.

Fermat donne un exposant 10, qui divise 100.

Revenir à la recherche, p. 10

Suivre l'exponentiation rapide

Indice 1 — Une piste.

L'exposant est impair : commence par transférer un facteur b dans r.

Indice 2 — Un pas de plus.

Ensuite b est mis au carré modulo 7 et e est divisé par deux.

Revenir à la recherche, p. 11

Décrire des diviseurs carrés

Indice 1 — Une piste.

Décompose 72 en facteurs premiers.

Indice 2 — Un pas de plus.

Dans $72 = 2^3 \times 3^2$, garde seulement des exposants pairs.

Revenir à la recherche, p. 12

Réfuter un mauvais usage de Fermat

Indice 1 — Une piste.

Le module 9 est-il premier ?

Indice 2 — Un pas de plus.

Calcule 2^6 modulo 9 puis multiplie par 2^2.

Revenir à la recherche, p. 13

Fermat et factorisation dans le même calcul

Indice 1 — Une piste.

Les modules 3 et 5 sont premiers et ne divisent pas 2.

Indice 2 — Un pas de plus.

Fermat donne $2^2 \equiv 1 \pmod 3$ et $2^4 \equiv 1 \pmod 5$.

Revenir à la recherche, p. 24

13 Explications des pauses et des preuves

Lis une étape, puis essaie de poursuivre avant de lire la suivante. Les calculs ci-dessous complètent le cours.

Une preuve de primalité doit finir les essais

$10^2 = 100 < 101 < 121 = 11^2$, donc les premiers au plus égaux à la racine sont 2,3,5,7. Le nombre 101 est impair ; sa somme de chiffres vaut 2, non multiple de 3 ; il ne finit ni par 0 ni par 5 ; et $101 = 7 \times 14 + 3$, donc 7 ne le divise pas. Tous les premiers possibles sous la borne ont été exclus. Si 101 était composé, le critère lui donnerait un diviseur premier dans cette liste, contradiction. Donc 101 est premier.

Revenir à la recherche, p. 5

Un premier divise un produit

Si $p \mid a$, l'une des deux conclusions est déjà vraie. Sinon, les diviseurs communs positifs de p et a ne peuvent être que 1 ou p, puisque p est premier. Le second est exclu par l'hypothèse $p \nmid a$, donc $\gcd(p, a) = 1$. Gauss appliqué à $p \mid ab$ permet alors de supprimer le facteur a et donne $p \mid b$. Ces deux cas couvrent toutes les possibilités. Pour un nombre composé comme 6, $6 \mid 2 \times 3$ alors que 6 ne divise aucun des deux facteurs : l'hypothèse « premier » est indispensable.

Revenir à la recherche, p. 6

Ce que prouve le produit plus un

$N = 2 \times 3 \times 5 + 1 = 31$. Chacun des nombres 2,3,5 divise 30. S'il divisait aussi 31, il diviserait $31 - 30 = 1$, impossible pour un entier supérieur à 1. Aucun ne divise donc N. Tout diviseur premier de N est nécessairement nouveau par rapport à la liste. Dans ce petit cas, $N = 31$ est lui-même premier, mais la preuve générale n'en a pas besoin : un N composé aurait aussi au moins un facteur premier, forcément absent de la liste.

Revenir à la recherche, p. 6

Une écriture vraiment première

L'égalité proposée est correcte, mais 45 n'est pas premier : $45 = 3 \times 15 = 3^2 \times 5$. En remplaçant, $540 = 2^2 \times 3 \times 3^2 \times 5 = 2^2 \times 3^3 \times 5$. Les exposants de 3 s'ajoutent parce que l'on multiplie un facteur 3 par deux autres facteurs 3. Tous les facteurs de base sont maintenant premiers. Le contrôle $4 \times 27 \times 5 = 108 \times 5 = 540$ vérifie le résultat ; il ne reste plus de facteur composé à décomposer.

Revenir à la recherche, p. 7

Compter sans oublier le diviseur 1

$72 = 2^3 \times 3^2$. Un diviseur est $2^a 3^b$ avec $a = 0, 1, 2, 3$ et $b = 0, 1, 2$. Il y a donc $4 \times 3 = 12$ choix, tous distincts. Pour un carré, chacun des deux exposants doit être pair. On garde $a = 0$ ou 2 et $b = 0$ ou 2 : quatre couples. Ils donnent $2^0 3^0 = 1$, $2^2 3^0 = 4$, $2^0 3^2 = 9$ et $2^2 3^2 = 36$. Chacun divise 72, et leurs racines entières sont 1,2,3,6.

Revenir à la recherche, p. 8

Vérifier les hypothèses

11 est premier. La base 6 n'est pas divisible par 11, donc Fermat donne bien $6^{11-1} = 6^{10} \equiv 1 \pmod{11}$. Pour la base 11, la deuxième hypothèse échoue : 11^{10} contient un facteur 11 et a pour reste 0, pas 1. La version $a^{11} \equiv a$ reste vraie dans les deux cas ; pour $a = 11$, ses deux membres ont reste zéro. Il ne faut donc pas simplifier cette version par une base non inversible.

Revenir à la recherche, p. 10

Réduire le bon exposant

Le nombre 11 est premier et ne divise pas 2. Fermat donne donc $2^{10} \equiv 1 \pmod{11}$. Comme $100 = 10 \times 10$, $2^{100} = (2^{10})^{10} \equiv 1^{10} = 1$. Ce nombre est entre 0 et 10, donc c'est le reste demandé. Les valeurs sont réduites modulo 11, tandis que le regroupement de l'exposant utilise 10. Cette différence vient précisément de l'exposant $p - 1$ dans le théorème.

Revenir à la recherche, p. 10

Suivre l'exponentiation rapide

Le triplet initial est $(1, 3, 13)$. Comme 13 est impair, le code remplace r par $1 \times 3 \bmod 7 = 3$. Puis il remplace b par $3^2 \bmod 7 = 9 \bmod 7 = 2$, et e par $13//2 = 6$. Le triplet est donc $(3, 2, 6)$. L'identité exacte $3^{13} = 3(3^2)^6$ explique le transfert d'un facteur puis la division de l'exposant. Modulo 7, elle devient $3^{13} \equiv 3 \times 2^6$. Or $2^3 = 8 \equiv 1$, donc le produit a reste 3 : l'invariant est bien conservé.

Revenir à la recherche, p. 11

Décrire des diviseurs carrés

$72 = 2^3 \times 3^2$. Tout diviseur positif s'écrit $2^a 3^b$ avec $0 \leq a \leq 3$ et $0 \leq b \leq 2$. Pour être un carré, il doit avoir a, b pairs. Les seuls choix sont $(0,0), (2,0), (0,2), (2,2)$, donnant 1,4,9,36. Ils sont bien des carrés $(1^2, 2^2, 3^2, 6^2)$ et divisent 72. Aucune autre paire d'exposants pairs n'est disponible, donc la liste est complète.

Revenir à la recherche, p. 12

Réfuter un mauvais usage de Fermat

Le module 9 vaut 3^2, donc n'est pas premier. Fermat ne garantit rien avec l'exposant $9-1$. Calculons : $2^6 = 64 = 7 \times 9 + 1$, donc $2^6 \equiv 1$. Puis $2^8 = 2^6 \times 2^2 \equiv 1 \times 4 = 4 \pmod 9$. Le reste 4 réfute l'affirmation proposée. La base 2 est pourtant première avec 9 ; même cette propriété ne permet pas d'utiliser la conclusion de Fermat avec un module composé.

Revenir à la recherche, p. 13

Fermat et factorisation dans le même calcul

Modulo 3, Fermat s'applique puisque 3 est premier et ne divise pas 2 : $2^2 \equiv 1$, donc $2^{20} = (2^2)^{10} \equiv 1$. Modulo 5, les mêmes hypothèses sont vérifiées : $2^4 \equiv 1$, donc $2^{20} = (2^4)^5 \equiv 1$. Ainsi 3 et 5 divisent $D = 2^{20} - 1$. Écrivons $D = 3k$; comme $5 \mid 3k$ et $\gcd(5,3) = 1$, $5 \mid k$, donc $15 \mid D$. Le reste de 2^{20} modulo 15 est donc 1. Fermat a été appliqué aux deux premiers, pas au module composé 15.

Revenir à la recherche, p. 24