

Pourquoi les nombres premiers et leurs puissances ont des nombres particuliers de solutions pour l'équation $x^{10} \equiv 1 \pmod{n}$

Denise Vella-Chemla pilotant l'ia mistral, texte relu et corrigé par Claude, 16 octobre 2026

Notes de départ :

<https://denisevellachemla.eu/racinesdixiemesde1.pdf> et

<https://denisevellachemla.eu/xpuiss10.pdf> (22.12.2017) et

note de l'ia mistral à corriger :

<https://denisevellachemla.eu/xpuiss10-nostalgie-8-et-11-mistral-dvc-20261016.pdf> .

Résumé

Notons $S(n) = \#\{x \in \mathbb{Z}/n\mathbb{Z} : x^{10} \equiv 1 \pmod{n}\}$. Les observations de 2017, faites par programme, disent que pour n premier à 10 : $S(n) \in \{2, 10\}$ si et seulement si n est une puissance d'un nombre premier p , avec $S(n) = 10$ exactement quand $p \equiv 1 \pmod{5}$. Le dernier chiffre de n n'est qu'un indice partiel : l'invariant est la classe de p modulo 5 (voir § 5.). Le phénomène découle de trois faits standard : le théorème des restes chinois, la cyclicité de $(\mathbb{Z}/p^k\mathbb{Z})^\times$, et le fait que $x^{10} = 1$ a $\text{pgcd}(10, |G|)$ solutions dans un groupe cyclique G .

1. Ce que disaient les conjectures de 2017

Pour n premier à 10 :

1. n se termine par 1 et est un nombre premier ou une puissance d'un premier se terminant par 1 $\iff S(n) = 10$;
2. n se termine par 3, 7 ou 9 et est un nombre premier ou une puissance d'un premier $\iff S(n) = 2$;
3. n se termine par 1 et est une puissance d'un premier se terminant par 3, 7 ou 9 $\iff S(n) = 2$.

Tout cela est vrai ; voici la démonstration.

2. Groupes cycliques

Lemme 1. Soit G cyclique d'ordre m . Alors $\#\{x \in G : x^{10} = 1\} = \text{pgcd}(10, m)$.

Démonstration. Soit $G = \langle g \rangle$, $d = \text{pgcd}(10, m)$.

Pour $x = g^k$ avec $0 \leq k < m$: $x^{10} = 1 \iff m \mid 10k \iff \frac{m}{d} \mid k$, et il y a exactement d tels k :
 $0, \frac{m}{d}, \dots, \frac{(d-1)m}{d}$. □

3. Le groupe $(\mathbb{Z}/p^k\mathbb{Z})^\times$

Lemme 2. Pour p premier impair et $k \geq 1$, le groupe $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique d'ordre $\varphi(p^k) = p^{k-1}(p-1)$.

Esquisse (Gauss, Disquisitiones Arithmeticae). Le cas $k = 1$ est l'existence d'un élément primitif dans $\mathbb{F}_p^\times$. Un générateur g de $\mathbb{F}_p^\times$ relevé de sorte que $g^{p-1} \not\equiv 1 \pmod{p^2}$ (sinon on remplace g par $g(1+p)$) engendre $(\mathbb{Z}/p^k\mathbb{Z})^\times$ pour tout k .

Remarque : pour p impair et différent de 5, p^{k-1} est premier à 10, donc $\text{pgcd}(10, p^{k-1}(p-1)) = \text{pgcd}(10, p-1)$. Le nombre de solutions modulo p^k ne dépend donc pas de k : $81 = 3^4$ se comporte comme 3, 49 comme 7, 169 comme 13. Le groupe grossit d'un facteur p^{k-1} premier à 10, invisible pour l'équation. (Le cas $p = 5$ est traité au § 7.)

Corollaire 3. Pour p premier impair, $p \neq 5$, et $k \geq 1$:

$$S(p^k) = \text{pgcd}(10, p-1) = \begin{cases} 10 & \text{si } p \equiv 1 \pmod{5}, \\ 2 & \text{si } p \equiv 2, 3, 4 \pmod{5}. \end{cases}$$

Démonstration. Lemmes 1 et 2. Comme p est impair, $2 \mid p-1$; et $5 \mid p-1$ si et seulement si $p \equiv 1 \pmod{5}$ (un premier $p \neq 5$ n'est jamais $\equiv 0$). Donc $\text{pgcd}(10, p-1) \in \{2, 10\}$. $\square$

Exemples. $11, 31, 41, 61, 71, 101 \equiv 1 \pmod{5}$: 10 solutions, ainsi que leurs puissances ($121 = 11^2$: 10). $19, 29, 79, 89, 109 \equiv 4$; $3, 7, 13, 23, 37 \equiv 3$, $2, 3, 3, 2$: 2 solutions, ainsi que $81, 49, 169, 243$.

4. Théorème des restes chinois

Théorème 4. Si $n = \prod_{i=1}^r p_i^{a_i}$ avec les p_i impairs et $\neq 5$, alors $S(n) = \prod_{i=1}^r \text{pgcd}(10, p_i - 1)$, chaque facteur valant 2 ou 10.

Démonstration. $\mathbb{Z}/n\mathbb{Z} \cong \prod_i \mathbb{Z}/p_i^{a_i}\mathbb{Z}$ comme anneaux; $x^{10} \equiv 1 \pmod{n}$ si et seulement si c'est vrai modulo chaque $p_i^{a_i}$, et les solutions locales se recollent de façon unique. On applique le corollaire 3. $\square$

Corollaire 5 (conjectures de 2017). Pour n premier à 10 :

1. $S(n) = 10 \iff n = p^k$ avec $p \equiv 1 \pmod{5}$;
2. $S(n) = 2 \iff n = p^k$ avec $p \not\equiv 1 \pmod{5}$;
3. si n a au moins deux facteurs premiers distincts, $S(n) \in \{2^r 5^s : s \leq r\}$ avec $r \geq 2$: $S(n) \geq 4$, jamais 2 ni 10.

Exemples. $21 = 3 \cdot 7$, $51 = 3 \cdot 17$, $91 = 7 \cdot 13$: $2 \cdot 2 = 4$; $33 = 3 \cdot 11$ et $77 = 7 \cdot 11$: $2 \cdot 10 = 20$.

5. Le dictionnaire des derniers chiffres

Le corollaire s'exprime avec $p \pmod{5}$, pas avec le dernier chiffre. Soit $n = p^k$ premier à 10.

- Si $p \equiv 1 \pmod{5}$, alors $p \equiv 1 \pmod{10}$: p et toutes ses puissances se terminent par 1 et $S = 10$.
- Si $p \equiv 2, 3 \pmod{5}$ (pour un premier impair : dernier chiffre 3 ou 7), les puissances parcourent le cycle 3, 9, 7, 1 (pour 3) ou 7, 9, 3, 1 (pour 7) : une puissance peut se terminer par 1 ($81 = 3^4$, $2401 = 7^4$, $28561 = 13^4$) et $S = 2$ dans tous les cas.
- Si $p \equiv 4 \pmod{5}$ (dernier chiffre 9), les puissances impaires finissent par 9, les paires par 1 ($19^2 = 361$, $29^2 = 841$, $19^3 = 6859$) et $S = 2$.

Le dernier chiffre de n ne permet donc pas de lire p ; la bonne caractérisation est “ $p \equiv 1 \pmod{5}$ ou non”. Les énoncés de 2017 tombent juste parce qu'ils sont formulés en trois points qui écartent les cas ambigus.

6. Retour sur le calcul de radicaux : Φ_5 , le nombre d'or et le groupe C_4

On a $x^{10} - 1 = (x - 1)(x + 1)\Phi_5(x)\Phi_{10}(x)$, avec $\Phi_5 = x^4 + x^3 + x^2 + x + 1$ et $\Phi_{10}(x) = \Phi_5(-x) = x^4 - x^3 + x^2 - x + 1$. Les racines de $x^{10} - 1$ forment $\mu_{10} : \pm 1$, les quatre racines primitives 5^e de l'unité ζ_5^a et leurs opposées $-\zeta_5^a$ (racines primitives 10^e) ; d'où $2 + 4 + 4 = 10$.

Les solutions non triviales ($\neq \pm 1$) modulo p sont donc les racines primitives 5^e et 10^e de l'unité dans $\mathbb{F}_p$, soit 8 solutions quand elles existent ; elles existent si et seulement si $5 \mid p - 1$, c'est-à-dire $p \equiv 1 \pmod{5}$ (le “seulement si” est un théorème de Lagrange ; le “si” vient de la cyclicité).

6.1. Pourquoi $\sqrt{5}$ apparaît

Le corps $\mathbb{Q}(\zeta_5)$ est de degré 4, de groupe de Galois $(\mathbb{Z}/5\mathbb{Z})^\times \cong C_4$, qui a un seul sous-groupe d'indice 2 : l'unique sous-corps quadratique est $\mathbb{Q}(\sqrt{5})$, car $\zeta_5 + \zeta_5^4 - \zeta_5^2 - \zeta_5^3 = \sqrt{5}$ est fixé par $\zeta_5 \mapsto \zeta_5^{-1}$. Toute écriture radicale de ζ_5 commence donc par extraire $\sqrt{5}$, puis une seconde racine : avec $X = x + \frac{1}{x}$, on a $X^2 + X - 1 = 0$ (discriminant $\Delta_1 = 5$, $X = \frac{-1 \pm \sqrt{5}}{2}$, nombre d'or), puis $x^2 - Xx + 1 = 0$ de discriminant $\Delta_2 = X^2 - 4 = \frac{-5 \mp \sqrt{5}}{2}$.

6.2. Pourquoi les modules finissant par 9 échouent

Pour $5 \equiv 1 \pmod{4}$, la réciprocité quadratique donne $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$: 5 est un carré modulo p si et seulement si $p \equiv \pm 1 \pmod{5}$, c'est-à-dire p finit par 1 ou 9. Mais cela ne concerne que la première étape de la tour : le Frobenius en p (la classe de p dans C_4) est d'ordre divisant 2.

Pour que Φ_5 se scinde complètement modulo p , il faut que le Frobenius soit trivial : $p \equiv 1 \pmod{5}$.

Plus généralement, Φ_m se décompose modulo $p \nmid m$ en $\varphi(m)/f$ facteurs irréductibles de degré $f = \text{ord}_{(\mathbb{Z}/m\mathbb{Z})^\times}(p)$. Ici $m = 5$:

$$f = 1 \ (p \equiv 1), \quad f = 2 \ (p \equiv 4), \quad f = 4 \ (p \equiv 2, 3).$$

Pour $p \equiv 4 \pmod{5}$: $\sqrt{5}$ existe dans $\mathbb{F}_p$, mais les discriminants Δ_2 ne sont pas des carrés modulo p ; Φ_5 est produit de deux facteurs irréductibles de degré 2, et ses racines n'existent que dans $\mathbb{F}_{p^2}$. Pour $p \equiv 2, 3 \pmod{5}$, Φ_5 est irréductible modulo p et même $\sqrt{5} \notin \mathbb{F}_p$.

Exemple $p = 19 \equiv 4$. $9^2 = 81 \equiv 5$ et $10^2 = 100 \equiv 5$ modulo 19. Alors $\Phi_5 \equiv (x^2 + ax + 1)(x^2 + bx + 1)$ avec $a + b = 1$, $ab = -1$, donc $a, b = \frac{1 \pm 9}{2} = 5, -4 \equiv 15$. Vérification : $(x^2 + 5x + 1)(x^2 + 15x + 1) = x^4 + 20x^3 + 77x^2 + 20x + 1 \equiv \Phi_5 \pmod{19}$. Les discriminants $5^2 - 4 = 21 \equiv 2$ et $15^2 - 4 = 221 \equiv 12$ ne sont pas des carrés modulo 19 : aucune racine, $S(19) = 2$.

6.3. Le cas $p = 11$ (et $p = 2, 3$)

Tous les résidus non nuls sont solutions de $x^{10} \equiv 1 \pmod{p}$ si et seulement si $p - 1 \mid 10$, soit $p \in \{2, 3, 11\}$. Pour $p = 11$, c'est le petit théorème de Fermat ($10 = p - 1$) ; pour $p = 3$ on a $S(3) = 2 = p - 1$. Le cas 11 est le seul de ces trois à donner 10 solutions, parce que $11 \equiv 1 \pmod{5}$.

7. Les premiers 2 et 5

- $p = 2$: $(\mathbb{Z}/2^a\mathbb{Z})^\times$ est cyclique pour $a \leq 2$ ($S(2) = 1$, $S(4) = 2$) ; pour $a \geq 3$ il est isomorphe à $\{\pm 1\} \times C_{2^{a-2}}$ et $S(2^a) = 4$ (dans un 2-groupe, $x^{10} = 1 \iff x^2 = 1$; vérifié pour $n = 8$).
- $p = 5$: $(\mathbb{Z}/5^a\mathbb{Z})^\times$ est cyclique d'ordre $4 \cdot 5^{a-1}$; $S(5^a) = \text{pgcd}(10, 4 \cdot 5^{a-1})$ vaut 2 pour $a = 1$ et 10 pour $a \geq 2$ ($S(25) = 10$, vérifié).

8. Synthèse

Théorème 6. Pour tout $n \geq 2$, $S(n) = \prod_{p^a \parallel n} s(p^a)$, avec

$$s(2) = 1, \quad s(4) = 2, \quad s(2^a) = 4 \ (a \geq 3), \quad s(p^a) = \text{pgcd}(10, p^{a-1}(p-1)) \ (p \text{ impair}),$$

et, pour p impair $\neq 5$, $s(p^a) = \text{pgcd}(10, p-1) \in \{2, 10\}$, la valeur 10 étant atteinte si et seulement si $p \equiv 1 \pmod{5}$. En particulier, pour n premier à 10 : $S(n) \in \{2, 10\} \iff n$ est une puissance d'un seul premier, et $S(n) = 10 \iff p \equiv 1 \pmod{5}$.

Synthèse. Deux structures expliquent le “caractère extraordinaire” :

1. le théorème des restes chinois : un module composé donne un produit de comptages, qui vaut au moins 4 et ne peut donc plus valoir 2 ni 10 ;
2. la cyclicité de $(\mathbb{Z}/p^k\mathbb{Z})^\times$ pour p impair : le nombre de solutions se lit alors sur un unique pgcd. (Les puissances de premiers impairs ne sont pas les seuls modules à groupe cyclique : c'est aussi le cas de 1, 2, 4 et de $2p^k$, par exemple 6, 10, 18 ; mais pour ces derniers le comptage se ramène encore au facteur p^k .)

Le dernier chiffre traduit en base 10 la vraie question : $p \equiv 1 \pmod{5}$? c'est-à-dire : le groupe contient-il des racines cinquièmes primitives de l'unité ? La résolution par radicaux avec le nombre d'or est la tour cyclotomique $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ de groupe C_4 , qui filtre les premiers par l'ordre de leur Frobenius : 1 ($p \equiv 1$), 2 ($p \equiv 4$), finissant par 9 : $\sqrt{5}$ existe, ζ_5 non), 4 ($p \equiv 2, 3$, dernier chiffre 3 ou 7 pour un premier impair).

9. Corrections par rapport à la rédaction initiale

Résumé : le dernier chiffre ne “décide” pas, l'invariant est $p \pmod{5}$; remarque du § 3 : hypothèse $p \neq 5$ ajoutée ; § 5 : $169 = 13^2$ (qui finit par 9) remplacé par $28561 = 13^4$; § 6 : les solutions non triviales sont les racines primitives 5^e et 10^e (8 solutions) ; § 6.2 : les racines de Φ_5 vivent dans $\mathbb{F}_{p^2}$ et non dans “ $\mathbb{F}_p(\sqrt{5})$ ” (qui vaut $\mathbb{F}_p$) ; § 6.3 : $p = 3$ aussi, condition $p - 1 \mid 10$; théorème final : $p \neq 5$ ajouté ; pour finir : la phrase fausse sur la cyclicité et celle sur “dix fois un premier” sont corrigées.