

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

Je fournis à l'ia mistral les deux notes ci-dessous et lui demande de me fournir les explications de ces nombres de solutions particuliers.

[1] <https://denisevellachemla.eu/racinesdixiemesde1.pdf>

[2] <https://denisevellachemla.eu/xpuiss10.pdf>

L'intégralité de la suite de cette note a été rédigée par l'ia mistral.

Résumé

Dans deux notes du 22.12.2017 [1] et [2], tu avais constaté par programme une caractérisation “rigolote” : le nombre de solutions de $x^{10} \equiv 1 \pmod{n}$, pour n ni divisible par 2 ni divisible par 5, vaut exactement 10 ou exactement 2 si et seulement si n est une puissance d'un nombre premier, et le dernier chiffre de n décide lequel. Ce document explique *pourquoi* : le phénomène est une conséquence complète et élémentaire de trois faits standard

1. le théorème des restes chinois,
2. la cyclicité du groupe $(\mathbb{Z}/p^k\mathbb{Z})^\times$,
3. et le lemme élémentaire “l'équation $x^{10} = 1$ a $\text{pgcd}(10, |G|)$ solutions dans un groupe cyclique”.

L'invariant caché n'est pas le dernier chiffre de n mais le résidu modulaire de n selon l'unique nombre premier p tel que $n = p^k$. On explique aussi pourquoi ton calcul de radicaux $\sqrt{5}$, $\sqrt{-\sqrt{5}}\varphi$, etc. fonctionne, et pourquoi il échoue précisément pour les modules se terminant par 9 alors que 5 y est pourtant un carré - question que tu laissais ouverte dans [2].

1. Ce que disaient tes conjectures de 2017

Notons

$$S(n) = \#\{x \in \mathbb{Z}/n\mathbb{Z} : x^{10} \equiv 1 \pmod{n}\}.$$

Tes observations de résultats d'exécution de programmes étaient (pour n premier à 10) :

- un nombre n qui se termine par 1 est un nombre premier ou une puissance d'un nombre premier se terminant par un 1 si et seulement si l'équation modulaire $x^{10} \equiv 1 \pmod{n}$ a exactement 10 solutions ;
- un nombre n qui se termine par 3, 7 ou 9 est un nombre premier ou une puissance d'un nombre premier (se terminant par 3, 7, ou 9) si et seulement si l'équation modulaire $x^{10} \equiv 1 \pmod{n}$ a exactement 2 solutions ;
- un nombre n qui se termine par 1 est une puissance d'un nombre premier se terminant par 3, 7, ou 9 si et seulement si l'équation modulaire $x^{10} \equiv 1 \pmod{n}$ a exactement 2 solutions.

Tout cela est vrai, et tout cela n'est que le résultat d'un théorème de structure des groupes multiplicatifs $(\mathbb{Z}/n\mathbb{Z})^\times$. Voici la démonstration complète.

2. Dans un groupe cyclique d'ordre m , l'équation $x^{10} = 1$ a $\text{pgcd}(10, m)$ solutions.

Lemme 1. Soit G un groupe cyclique d'ordre m (noté multiplicativement). Alors

$$\#\{x \in G : x^{10} = 1 \text{ dans } G\} = \text{pgcd}(10, m).$$

Démonstration. Écrivons $G = \langle g \rangle$, $|G| = m$, et soit $d = \text{pgcd}(10, m)$. Un élément $x = g^k$ vérifie $x^{10} = 1$ si et seulement si $g^{10k} = 1$, c'est-à-dire $m \mid 10k$.

L'entier $k \in \{0, \dots, m-1\}$ vérifie $m \mid 10k$ si et seulement si $\frac{m}{d} \mid k$, et il y a exactement d tels k dans $\{0, \dots, m-1\}$, à savoir $0, \frac{m}{d}, \frac{2m}{d}, \dots, \frac{(d-1)m}{d}$.

(En langage des ordres : l'ordre de x divise 10 et divise m , donc divise $\text{pgcd}(10, m) = d$; Un groupe cyclique d'ordre n possède exactement $\varphi(d)$ éléments d'ordre d pour chaque diviseur d de n . $\square$)

C'est ce lemme trivial qui explique tous les comptages. La seule chose qu'il faut savoir en plus est *quel est l'ordre* du groupe dans lequel on résout l'équation, et *qu'il est cyclique*.

3. Le groupe $(\mathbb{Z}/p^k\mathbb{Z})^\times$: cyclique, d'ordre $p^{k-1}(p-1)$

Lemme 2. Soit p un nombre premier impair et $k \geq 1$. Alors le groupe multiplicatif $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique, d'ordre

$$\varphi(p^k) = p^{k-1}(p-1).$$

Esquisse (fait classique). Le cas $k = 1$ est le théorème de l'élément primitif pour les corps finis : $(\mathbb{F}_p)^\times$ est cyclique d'ordre $p-1$ (Dans un groupe abélien fini G d'ordre N , il existe toujours un élément dont l'ordre est égal au PPCM des ordres de tous les éléments du groupe. On appelle cet ordre maximal l'exposant m du groupe). Pour passer de p à p^k : un générateur g de $(\mathbb{F}_p)^\times$ dont $g^{p-1} \not\equiv 1 \pmod{p^2}$ engendre déjà $(\mathbb{Z}/p^k\mathbb{Z})^\times$ pour tout k (sinon $g(1+p)$ le fait), d'où la cyclicité et l'ordre $p^{k-1}(p-1)$. C'est un résultat de Gauss (Disquisitiones, art. 85-91). $\square$

Remarque : pour p impair et $k \geq 1$, comme p^{k-1} est premier à 10,

$$\text{pgcd}(10, p^{k-1}(p-1)) = \text{pgcd}(10, p-1).$$

Conséquence capitale : le nombre de solutions modulo p^k ne dépend pas de k , il ne dépend que de p . C'est l'explication de ton point 3 : $81 = 3^4$ se comporte comme 3, 49 comme 7, 169 comme 13. Les puissances d'un premier ne créent aucune solution nouvelle, ni n'en détruisent : le groupe grossit ($p^{k-1}(p-1)$ éléments) mais grossit par un facteur p^{k-1} premier à 10, invisible pour l'équation $x^{10} \equiv 1 \pmod{p^k}$.

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. Combiner les lemmes 1 et 2. Le calcul de $\text{pgcd}(10, p-1)$: p est impair donc $2 \mid p-1$, et $5 \mid p-1$ si et seulement si $p \equiv 1 \pmod{5}$ (un premier $p \neq 5$ n'est jamais $\equiv 0 \pmod{5}$). Donc $\text{pgcd}(10, p-1) \in \{2, 10\}$, et il vaut 10 exactement quand $p \equiv 1 \pmod{5}$. $\square$

Exemples :

- $\rightarrow 11, 31, 41, 61, 71, 101 \equiv 1 \pmod{5}$: chacun donne 10 solutions, et leurs puissances aussi ($121 = 11^2 \rightarrow 10$ solutions, vérifié).
- $\rightarrow 19, 29, 79, 89, 109 \equiv 4, 4, 4, 4, 4 \pmod{5}$: 2 solutions.
- $\rightarrow 3, 7, 13, 23, 37 \equiv 3, 2, 3, 3, 2 \pmod{5}$: 2 solutions, et
- $\rightarrow 81 = 3^4, 49 = 7^2, 169 = 13^2, 243 = 3^5$: 2 solutions.

4. Le théorème des restes chinois : les composés sont des produits

Théorème 4. Soit $n = \prod_{i=1}^r p_i^{a_i}$ la décomposition de n en facteurs premiers, avec tous les p_i impairs, $p_i \neq 5$. Alors

$$S(n) = \prod_{i=1}^r \text{pgcd}(10, p_i - 1) \quad (\text{chaque facteur vaut 2 ou 10}).$$

Démonstration. Par le théorème des restes chinois, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au produit $\prod_i \mathbb{Z}/p_i^{a_i}\mathbb{Z}$, et l'isomorphisme est un isomorphisme d'anneaux : $x^{10} \equiv 1 \pmod{n}$ si et seulement si $x^{10} \equiv 1$ modulo chaque $p_i^{a_i}$, et chaque solution locale se recolle de façon unique en une solution globale. Donc $S(n) = \prod_i S(p_i^{a_i}) = \prod_i \text{pgcd}(10, p_i - 1)$ par le corollaire 3. $\square$

Corollaire 5 (tes conjectures, démontrées). Avec 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, $S(n) = \prod_i \text{pgcd}(10, p_i - 1) \in \{4, 20, 100, \dots\}$
- un produit d'au moins deux facteurs chacun ≥ 2 , donc jamais 2 ni 10.

Démonstration. Chaque $\text{pgcd}(10, p_i - 1)$ vaut 2 ou 10. Si $r = 1$, n est une puissance d'un premier et on lit le corollaire 3. Si $r \geq 2$, le produit de $r \geq 2$ entiers appartenant à $\{2, 10\}$ est dans $\{4, 20, 100, \dots\} = \{2^r 5^s : s \leq r\}$, en particulier ≥ 4 : jamais 2, ni 10. $\square$

Exemples :

- $\rightarrow 21 = 3 \cdot 7 : \text{pgcd}(10, 2) \cdot \text{pgcd}(10, 6) = 2 \cdot 2 = 4.$
- $\rightarrow 51 = 3 \cdot 17 : 2 \cdot 2 = 4.$
- $\rightarrow 91 = 7 \cdot 13 : 2 \cdot 2 = 4.$
- $\rightarrow 33 = 3 \cdot 11 : 2 \cdot 10 = 20.$
- $\rightarrow 77 = 7 \cdot 11 : 2 \cdot 10 = 20.$

Tes annexes donnent bien 4 solutions pour 21, 51, 91.

5. Le dictionnaire des derniers chiffres

Le corollaire 5 est exprimé avec $p \pmod{5}$, pas avec le dernier chiffre. Pourquoi le dernier chiffre de n fonctionne quand même ? Faisons le dictionnaire. Soit $n = p^k$ premier à 10.

n se termine par 1. Alors $n \equiv 1 \pmod{5}$. Mais attention : $p^k \equiv 1 \pmod{5}$ n'implique pas $p \equiv 1 \pmod{5}$ - car $(\mathbb{Z}/5\mathbb{Z})^\times$ est un groupe d'ordre 4, et $p^k \equiv 1$ dès que $\text{ord}_{(\mathbb{Z}/5\mathbb{Z})^\times}(p)$ divise k : ainsi $81 = 3^4 \equiv 1 \pmod{5}$ alors que $3 \not\equiv 1 \pmod{5}$. C'est exactement ton point 3 : le dernier chiffre de n ne se lit pas sur p seul, il faut le dictionnaire complet :

- si $p \equiv 1 \pmod{5}$, alors p est impair et $\equiv 1 \pmod{5}$, donc $p \equiv 1 \pmod{10}$: p et toutes ses puissances se terminent par 1, et $S(p^k) = 10$;
- si $p \equiv 2$ ou $3 \pmod{5}$ (dernier chiffre 2, 3, 7, 8 ; pour un nombre premier : 3 ou 7), les puissances p^k se terminent en parcourant un cycle (3, 9, 7, 1 pour 3 ; 7, 9, 3, 1 pour 7) : une puissance peut se terminer par 1 ($81 = 3^4$, $2401 = 7^4$, ou $169 = 13^2$) et dans tous les cas $S(p^k) = 2$;
- si $p \equiv 4 \pmod{5}$ (dernier chiffre 9), $p^k \equiv 4$ ou $1 \pmod{5}$: les puissances impaires finissent par 9, les paires par 1 (ex. $19^2 = 361$, $29^2 = 841$, $19^3 = 6859$) et toujours $S(p^k) = 2$.

Autrement dit : le dernier chiffre de n ne se lit pas sur n seul, mais sur p . La bonne caractérisation est " $p \equiv 1 \pmod{5}$ ou non" ; le dernier chiffre de n n'est qu'une approximation partielle, qui tombe juste dans tes énoncés parce que " n finit par 1 et $n = p^k$ " écarte les cas ambigus au prix d'un énoncé en trois points.

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

Tu factorisais

$$x^{10} - 1 = (x - 1)(x + 1) \Phi_5(x) \Phi_{10}(x), \quad \Phi_5(x) = x^4 + x^3 + x^2 + x + 1, \quad \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

Les racines de $x^{10} - 1$ forment le groupe μ_{10} des racines 10-ièmes de l'unité ; celles de Φ_5 sont les racines primitives 5-ièmes ζ_5^a , $a = 1, 2, 3, 4$, et $\Phi_{10}(x) = \Phi_5(-x)$: ses racines sont $-\zeta_5^a$ - d'où ton observation que le polynôme alterné s'annule en $-x$ quand le polynôme simple s'annule en x .

Les solutions de $x^{10} \equiv 1$ non triviales modulo p sont donc exactement les racines primitives 5-ièmes de l'unité dans $\mathbb{F}_p$, et il en existe une (et alors quatre) si et seulement si 5 divise l'ordre du groupe $(\mathbb{F}_p)^\times$, c'est-à-dire $5 \mid p - 1$, i.e. $p \equiv 1 \pmod{5}$.

C'est une instance du critère de divisibilité de Lagrange : dans un groupe fini d'ordre m , il existe un élément d'ordre d si et seulement si $d \mid m$ (le "seulement si" est le critère de divisibilité de Lagrange ; le "si" exige la cyclicité, acquise ici). Aucun radical n'est nécessaire pour le voir : c'est la structure du groupe qui parle.

6.1. Pourquoi $\sqrt{5}$ apparaît dans la note [1]

Le corps de décomposition de Φ_5 sur $\mathbb{Q}$ est $\mathbb{Q}(\zeta_5)$, de degré $\varphi(5) = 4$, de groupe de Galois $(\mathbb{Z}/5\mathbb{Z})^\times \cong C_4$ - cyclique, comme le disait ton document. Un groupe cyclique d'ordre 4 a une seule sous-extension

quadratique, donc un seul sous-corps de degré 2 : c'est $\mathbb{Q}(\sqrt{5})$, car la somme de Gauss

$$\zeta_5 + \zeta_5^4 - \zeta_5^2 - \zeta_5^3 = \sqrt{5}$$

(liée au nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$, elle est fixée par l'involution $\zeta_5 \mapsto \zeta_5^{-1}$ de C_4 . Toute écriture radicale de ζ_5 commence donc par extraire $\sqrt{5}$, puis par une deuxième extraction : c'est exactement ta double équation du second degré

$$X = x + \frac{1}{x},$$

puis

$$x^2 - Xx + 1 = 0,$$

avec les discriminants

$$\Delta_1 = 5, \quad \Delta_2 = \frac{-5 \pm \sqrt{5}}{2} = -\sqrt{5} \frac{1 \pm \sqrt{5}}{2} \cdot (\pm 1),$$

dans laquelle tu reconnaissais le nombre d'or.

6.2. Pourquoi les modules finissant par 9 échouent : ta question ouverte de la référence [2]

Dans [2], tu notais : pour n finissant par 9, 5 possède bien deux racines carrées modulo n , et pourtant Φ_5 ne s'annule jamais - "il reste à comprendre pourquoi".

Voici l'explication.

La loi de réciprocité quadratique donne, puisque $5 \equiv 1 \pmod{4}$,

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right),$$

et comme les carrés modulo 5 sont 1 et 4 : 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 l'existence de $\sqrt{5}$ modulo p ne concerne que la *première étape* de la tour radicale ; elle dit seulement que le Frobenius en p (l'élément $p \pmod{5}$ du groupe de Galois C_4) a un ordre qui divise 2, i.e. $p \equiv \pm 1 \pmod{5}$.

Pour que Φ_5 se *scinde complètement* en facteurs linéaires modulo p - quatre racines -, il faut que le Frobenius soit *trivial*, c'est-à-dire

$$p \equiv 1 \pmod{5}.$$

Pour $p \equiv 4 \equiv -1 \pmod{5}$ (dernier chiffre 9), le Frobenius est l'involution $\zeta_5 \mapsto \zeta_5^{-1}$, d'ordre 2 : Φ_5 se factorise modulo p en *deux polynômes irréductibles de degré 2*, conjugués, sans aucune racine. C'est le sens profond du *théorème de décomposition des polynômes cyclotomiques* : Φ_m se scinde modulo p (premier à m) en $\varphi(m)/f$ facteurs irréductibles de degré f , où f est l'ordre de p dans $(\mathbb{Z}/m\mathbb{Z})^\times$.

Ici $m = 5$: $f = 1$ si $p \equiv 1 \pmod{5}$, $f = 2$ si $p \equiv 4 \pmod{5}$, $f = 4$ si $p \equiv 2, 3 \pmod{5}$.

Traduis dans ton langage : pour $p \equiv 4 \pmod{5}$, $\sqrt{5}$ existe bien, mais les discriminants intérieurs $\Delta_2 = \frac{-5 \pm \sqrt{5}}{2}$ ne sont *pas* des carrés modulo p - la deuxième extraction radicale échoue -, et les quatre solutions “existent” seulement sur l’extension quadratique $\mathbb{F}_p(\sqrt{5})$, pas dans $\mathbb{F}_p$ lui-même.

Pour $p \equiv 2, 3 \pmod{5}$ (dernier chiffre 2, 3, 7, 8), c’est pire : même $\sqrt{5}$ n’existe pas ($f = 4$, Φ_5 irréductible modulo p), et ton raisonnement de réciprocity le disait déjà.

Exemple [mod 19, dernier chiffre 9] : $19 \equiv 4 \pmod{5}$; 9 et 10 sont racines carrées de 5 modulo 19 (ton annexe 2). Ici $f = \text{ord}_{(\mathbb{Z}/5)^\times}(4) = 2$, donc

$$\Phi_5 \equiv (x^2 + ax + 1)(x^2 + bx + 1) \pmod{19}$$

avec $a + b = 1$, $ab + 2 = 1$, i.e. $ab = -1$: $a, b = \frac{1 \pm \sqrt{5}}{2}$ prennent les valeurs $\frac{1+9}{2} = 5$ et $\frac{1-9}{2} = -4 = 15$ modulo 19, et de fait

$$\begin{aligned} (x^2 + 5x + 1)(x^2 + 15x + 1) &= x^4 + 20x^3 + 77x^2 + 20x + 1 \\ &\equiv x^4 + x^3 + x^2 + x + 1 \pmod{19}. \end{aligned}$$

Aucun des deux polynômes quadratiques n’a de racine ($\Delta'_1 = 21 \equiv 2$, non carré ; $\Delta'_2 = 221 \equiv 12$, non carré modulo 19). Donc $S(19) = 2$ - conforme au programme.

6.3. Le miracle apparent $p = 11$

Modulo 11 : *tous* les résidus non nuls (1 à 10) sont solutions de $x^{10} \equiv 1$. C’est simplement le petit théorème de Fermat : $x^{10} \equiv 1 \pmod{11}$ pour tout x non multiple de 11. Le cas “tout le monde est solution” arrive pour $p = 11$ exactement parce que $10 = p - 1$; c’est le seul premier avec cette propriété, et il coïncide avec ta liste “10 solutions” car $11 \equiv 1 \pmod{5}$ et $p - 1 = 10 \mid$ chaque pgcd... en fait $S(11) = \text{pgcd}(10, 10) = 10$, formule générale.

7. Cas des premiers 2 et 5 (pour être complet)

- $p = 2$: $(\mathbb{Z}/2^a\mathbb{Z})^\times$ n’est cyclique que pour $a \leq 2$ ($a = 1$: trivial, $S(2) = 1$; $a = 2$: $\{\pm 1\}$, $S(4) = 2$) ; pour $a \geq 3$ il est isomorphe à $\{\pm 1\} \times C_{2^{a-2}}$, et alors $S(2^a) = 4$: les éléments d’ordre divisant 10 sont le produit d’un élément de $\{\pm 1\}$ (2 choix) par un élément de $C_{2^{a-2}}$ d’ordre divisant $\text{pgcd}(10, 2^{a-2}) = 2$ (2 choix) ; vérifié pour $n = 8$).
- $p = 5$: $(\mathbb{Z}/5^a\mathbb{Z})^\times$ est cyclique d’ordre $4 \cdot 5^{a-1}$; $S(5^a) = \text{pgcd}(10, 4 \cdot 5^{a-1})$, qui vaut 2 pour $a = 1$ et 10 pour $a \geq 2$ ($25 \rightarrow 10$ solutions, vérifié).

Ces cas n’ont rien d’exotique : même formule en $\text{pgcd}(10, \text{ordre du groupe})$, seule change la structure du groupe (produit pour 2^a , cyclique pour 5^a).

8. Synthèse

Théorème 6 (résumé final). *Pour tout $n \geq 2$:*

$$S(n) = \prod_{p^a \parallel n} s(p^a), \quad s(p^a) = \begin{cases} 1 & p = 2, a = 1, \\ 2 & p = 2, a = 2, \\ 4 & p = 2, a \geq 3, \\ \text{pgcd}(10, p^{a-1}(p-1)) & p \text{ impair}, \end{cases}$$

et pour p impair, $s(p^a) = \text{pgcd}(10, p-1) \in \{2, 10\}$, avec la valeur 10 si et seulement si $p \equiv 1 \pmod{5}$.

En particulier, pour n premier à 10 :

$$S(n) \in \{2, 10\} \iff n \text{ est une puissance d'un seul premier,}$$

$$S(n) = 10 \iff p \equiv 1 \pmod{5}.$$

Morale. Le caractère “extraordinaire” que tu ressentais - les premiers et leurs puissances sont les seuls modules donnant exactement 2 ou 10 solutions - est la trace, dans l'équation $x^{10} \equiv 1 \pmod{n}$, de deux structures fondamentales :

1. le *théorème des restes chinois* (composé = produit, donc les comptages se multiplient et ne peuvent plus être premiers ou dix fois un nombre premier)
2. et la *cyclicité de $(\mathbb{Z}/p^k\mathbb{Z})^\times$* (les premiers et leurs puissances sont les seuls modules dont le groupe multiplicatif est cyclique, si bien que le nombre de solutions se lit sur un unique pgcd).

Quant au rôle du dernier chiffre, il traduit en base 10 la vraie question arithmétique : *p est-il congru à 1 modulo 5 ?*, c'est-à-dire : *le groupe contient-il des racines cinquièmes primitives de l'unité ?* - et ta résolution par radicaux avec le nombre d'or était la décomposition de la tour cyclotomique $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ de groupe de Galois C_4 , filtrant les premiers selon l'ordre de leur Frobenius : 1 (finissant par 1), 2 (finissant par 9 : $\sqrt{5}$ existe, ζ_5 non), 4 (finissant par 2, 3, 7, 8).