

Nombre de solutions de l'équation $x^{10} \equiv 1 \pmod{n}$ en fonction du dernier chiffre de n (Denise Vella-Chemla, 22.12.2017)

Par programme, on a constaté les faits suivants que l'on énonce comme des conjectures :

- 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.

On a $x^{10} \equiv 1 \pmod{n} \iff x^{10} - 1 \equiv 0 \pmod{n}$.

Or $x^{10} - 1 = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$.

On oublie les solutions triviales 1 et $n - 1$ qui annulent, l'une, le monôme $x - 1$, et l'autre, le monôme $x + 1$. On oublie également le polynôme alterné $x^4 - x^3 + x^2 - x + 1$ car il s'annule pour $n - x$ lorsque le polynôme $x^4 + x^3 + x^2 + x + 1$ s'annule pour x et on se concentre donc sur l'annulation de ce polynôme simple symétrique $x^4 + x^3 + x^2 + x + 1$. On cherche pourquoi il s'annule 4 fois pour un nombre premier p se terminant par 1 ou une puissance de nombre premier p^k se terminant par 1 alors qu'il ne s'annule jamais pour un nombre premier p se terminant par 3, 7 ou 9 ou une puissance de nombre premier p^k se terminant par 3, 7 ou 9. On ne réfléchit pas pour l'instant au fait que modulo un nombre composé n , l'équation modulaire $x^{10} \equiv 1 \pmod{n}$ n'admet jamais 2 ou 10 solutions.

On résoud $x^4 + x^3 + x^2 + x + 1 = 0$ ainsi : on divise le polynôme par x^2 . On obtient :

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0$$

qu'on réécrit en :

$$\left(x^2 + \frac{1}{x^2}\right) + \left(x + \frac{1}{x}\right) + 1 = 0$$

(en mettant ensemble les premier et cinquième termes, ainsi que les second et quatrième termes).

On pose $X = x + \frac{1}{x}$.

L'équation se réécrit $X^2 + X - 1 = 0$. Le discriminant Δ_1 de cette nouvelle équation est égal à 5.

On a abouti aux 2 solutions suivantes pour X :

$$x + \frac{1}{x} = \frac{-1 \pm \sqrt{5}}{2}.$$

On multiplie les deux membres de l'égalité par x et on a à résoudre une autre équation du second degré :

$$x^2 + \frac{1 \pm \sqrt{5}}{2}x + 1 = 0$$

Le discriminant Δ_2 de cette seconde équation du second degré est égal à :

$$\Delta_2 = \frac{(1 \pm \sqrt{5})^2}{4} - 4 = \frac{1 \pm 2\sqrt{5} + 5 - 16}{4} = \frac{-5 \pm \sqrt{5}}{2}$$

Les deux solutions de cette seconde équation du second degré sont :

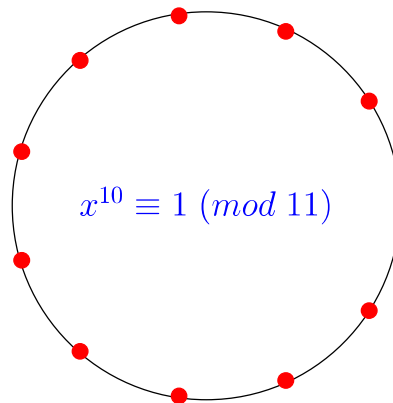
$$X = \frac{\frac{-1 \pm \sqrt{5}}{2} \pm \sqrt{\frac{-5 \pm \sqrt{5}}{2}}}{2}$$

Il n'y a aucune solution pour les nombres n de dernier chiffre 3 et 7 car modulo de tels nombres n , 5 n'est jamais un carré (i.e. n'a pas de racine carrée modulaire) dans $\mathbb{Z}/n\mathbb{Z}$.

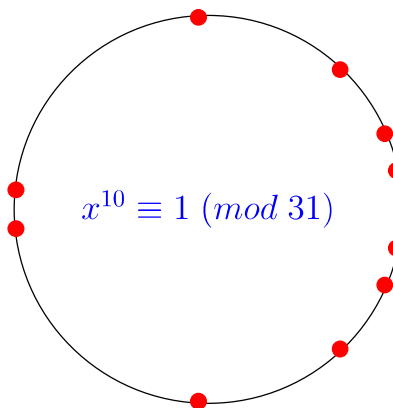
Mais pour les nombres n de dernier chiffre 1 ou 9, 5 admet toujours deux racines carrées (cf. annexe 2), il reste à comprendre pourquoi selon un module n de dernier chiffre 9, bien que 5 admette deux racines carrées modulaires, le polynôme $x^4 + x^3 + x^2 + x + 1$ ne peut cependant jamais être nul. Il faut aussi compléter le raisonnement pour les puissances d'un nombre premier plutôt que pour les nombres premiers simples.

Annexe 1 : Positionnement des solutions de l'équation $x^{10} \equiv 1 \pmod{p}$ sur cercles modulaires pour $p = 11, 31, 41, 61, 71$

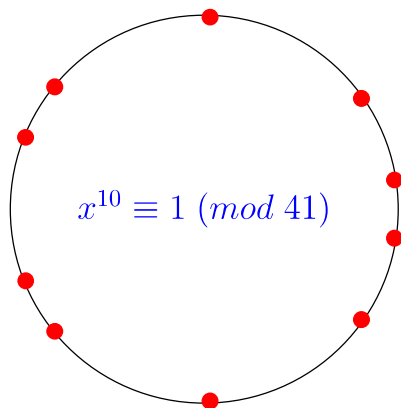
Solutions de $x^{10} \equiv 1 \pmod{11}$: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. 11 est premier. Il y a 10 solutions.



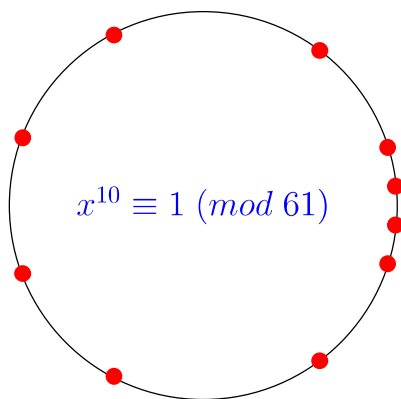
Solutions de $x^{10} \equiv 1 \pmod{31}$: 1, 2, 4, 8, 15, 16, 23, 27, 29, 30. 31 est premier. Il y a 10 solutions.



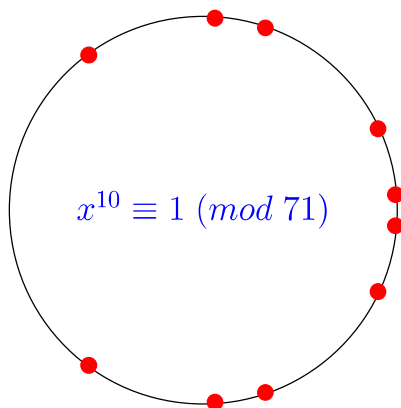
Solutions de $x^{10} \equiv 1 \pmod{41}$: 1, 4, 10, 16, 18, 23, 25, 31, 37, 40. 41 est premier. Il y a 10 solutions.



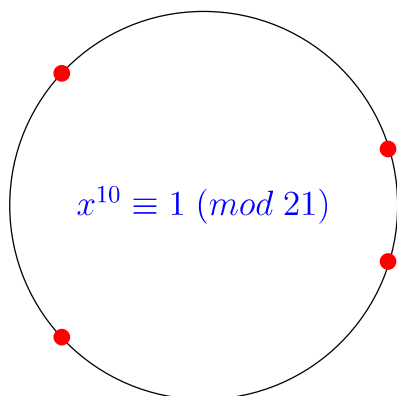
Solutions de $x^{10} \equiv 1 \pmod{61}$: 1, 3, 9, 20, 27, 34, 41, 52, 58, 60. 61 est premier. Il y a 10 solutions.



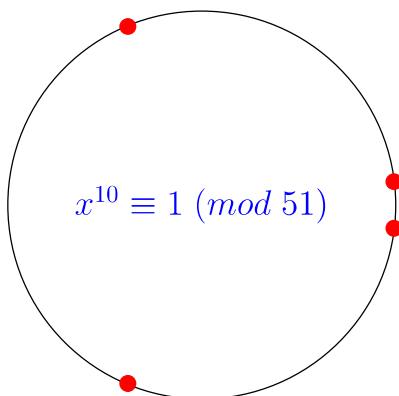
Solutions de $x^{10} \equiv 1 \pmod{71}$: 1, 5, 14, 17, 25, 46, 54, 57, 66, 70. 71 est premier. Il y a 10 solutions.



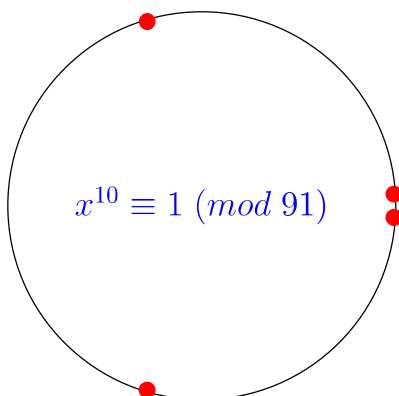
Solutions de $x^{10} \equiv 1 \pmod{21}$: 1, 8, 13, 20. 21 est composé. Il y a 4 solutions.



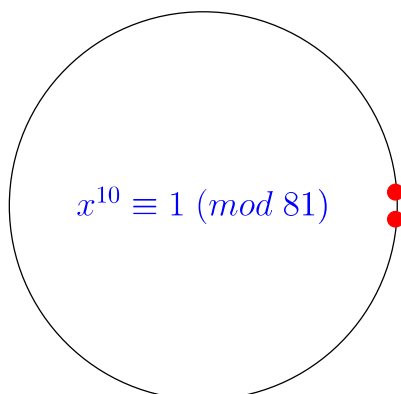
Solutions de $x^{10} \equiv 1 \pmod{51}$: 1, 16, 35, 50. 51 est composé. Il y a 4 solutions.



Solutions de $x^{10} \equiv 1 \pmod{91}$: 1, 27, 64, 90. 91 est composé. Il y a 4 solutions.



Solutions de $x^{10} \equiv 1 \pmod{81}$: 1, 80. 81 est composé, c'est une puissance d'un nombre premier se terminant par 3, l'équation n'a que deux solutions, les solutions triviales (de même par exemple, que l'équation $x^{10} \equiv 1 \pmod{49}$ (49 étant une puissance de 7), n'a que les deux solutions triviales 1 et 48).



Annexe 2 : Rappel des racines carrées modulaires de 5 pour les nombres n de dernier chiffre 1 ou 9 (obtenues par programme)

4 racine carrée de 5 (mod 11).

7 racine carrée de 5 (mod 11).

9 racine carrée de 5 (mod 19).

10 racine carrée de 5 (mod 19).

11 racine carrée de 5 (mod 29).

18 racine carrée de 5 (mod 29).

6 racine carrée de 5 (mod 31).

25 racine carrée de 5 (mod 31).

13 racine carrée de 5 (mod 41).

28 racine carrée de 5 (mod 41).

8 racine carrée de 5 (mod 59).

51 racine carrée de 5 (mod 59).

26 racine carrée de 5 (mod 61).

35 racine carrée de 5 (mod 61).

17 racine carrée de 5 (mod 71).

54 racine carrée de 5 (mod 71).

20 racine carrée de 5 (mod 79).

59 racine carrée de 5 (mod 79).

19 racine carrée de 5 (mod 89).

70 racine carrée de 5 (mod 89).