Nombre de solutions de l'équation $x^{10} \equiv 1\ (mod\ n)$ 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 $x^{10} \equiv 1\ (mod\ n)$ 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 $x^{10} \equiv 1\ (mod\ n)$ 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 $x^{10} \equiv 1\ (mod\ n)$ a exactement 2 solutions.

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

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 $1\ (mod\ n)$ et $-1\ (mod\ n)$ 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 $x^{10} \equiv 1\ (mod\ n)$ 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 obtient les 2 solutions suivantes pour X :

$$X_1 = x_1 + \frac{1}{x_1} = \frac{-1 + \sqrt{5}}{2}$$

et

$$X_2 = x_2 + \frac{1}{x_2} = \frac{-1 - \sqrt{5}}{2}.$$

Prenons l'équation de variable x_1. On multiplie les deux membres de la seconde égalité par x_1 et on a à résoudre une nouvelle équation du second degré :

$$x_1^2 - \frac{-1 + \sqrt{5}}{2} x_1 + 1 = 0$$

Le discriminant Δ_{21} de cette seconde équation du second degré est égal à :

$$\Delta_{21} = \left(\frac{1 - \sqrt{5}}{2}\right)^2 - 4 = \frac{1 - 2\sqrt{5} + 5 - 16}{4} = \frac{-5 - \sqrt{5}}{2} = -\sqrt{5}\left(\frac{1 + \sqrt{5}}{2}\right)$$

On reconnaît le nombre d'or φ.

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

$$x_1 = \frac{\frac{-1+\sqrt{5}}{2} \pm \sqrt{-\sqrt{5}\left(\frac{1+\sqrt{5}}{2}\right)}}{2}$$

On procède de même pour l'équation d'inconnue X_2. $\Delta_{22} = \sqrt{5}\left(\frac{1-\sqrt{5}}{2}\right)$ et on aboutit à :

$$x_2 = \frac{\frac{1+\sqrt{5}}{2} \pm \sqrt{\sqrt{5}\left(\frac{1-\sqrt{5}}{2}\right)}}{2}$$

On a ainsi l'explication du nombre exact de deux solutions (les seules solutions triviales 1 et -1) pour les nombres premiers se terminant par 3 ou 7 : il n'y a aucune solution à l'équation $x^4 + x^3 + x^2 + x + 1 \equiv 0\ (mod\ n)$ pour les nombres n de dernier chiffre 3, 7 car modulo de tels nombres, 5 n'est jamais un carré (i.e. n'a pas de racine carrée modulaire) dans $\mathbb{Z}/n\mathbb{Z}$ (5 est un $4k+1$, la loi de réciprocité quadratique entraîne que la relation de résiduosité quadratique qui lie 5 à un nombre est symétrique ($r(5,x) = r(x,5)$). Or 2 et 3 ne sont pas résidus quadratiques de 5 donc 5 n'est pas un carré pour tout nombre n de dernier chiffre 2 ou 7 ($\equiv 2\ (mod\ 5)$) ou 3 ou 8 ($\equiv 3\ (mod\ 5)$)[1].

Mais pour les nombres n de dernier chiffre 1 ou 9 ($\equiv 4\ (mod\ 5)$, donc résidu quadratique potentiel), 5 admet toujours deux racines carrées.

Voyons un exemple : modulo 11, prenons 4 qui est une des deux racines carrées de 5. La formule pour X_1 vaut :

$$\frac{\frac{-1+4}{2} \pm \sqrt{(-4)\left(\frac{1+4}{2}\right)}}{2} = \frac{\frac{3}{2} \pm \sqrt{-10}}{2}$$

Comme $-10 \equiv 1\ (mod\ 11)$, on trouve comme solutions $\frac{5}{4}$ qui vaut 4 et $\frac{1}{4}$ qui vaut 3.

La formule pour X_2 amène :

$$\frac{\frac{1+4}{2} \pm \sqrt{4\left(\frac{1-4}{2}\right)}}{2}.$$

Il faut alors avoir à l'esprit que $\frac{-3}{2} \equiv 4\ (mod\ 11)$. On a alors $\frac{\frac{5}{2} \pm 4}{2}$ qui vaut soit $\frac{\frac{13}{2}}{2} = \frac{2}{2} = \frac{1}{2} = 6$ ou $\frac{-3}{4} = 2$. Les nombres complémentaires à 11 des solutions trouvées 3, 4, 6 et 2 qui sont 8, 7, 5 et 9 sont racines de l'équation polynomiale alternée $x^4 - x^3 + x^2 - x + 1 = 0$. On peut aussi ne considérer que la seule équation polynomiale $x^4 + x^3 + x^2 + x + 1 = 0$ et voir que l'inverse d'une solution est aussi solution (par exemple, modulo 11, 2 et 16 sont inverses, 4 et 8 le sont également, ou encore 15 et 29, ou enfin 23 et 27). En ajoutant à l'ensemble des solutions les deux solutions triviales 1 et -1, on a bien 10 solutions exactement.

Des résolutions similaires pour les modules 31, 41, 61 et 71 sont fournies en annexe 2. On nous indique que le groupe de Galois de l'équation polynomiale $x^4 + x^3 + x^2 + x + 1 = 0$ est le groupe cyclique C_4. L'obtention d'une seule solution permet d'obtenir toutes les autres par élévation aux puissances successives d'une part et inversion d'autre part. Par exemple, une fois trouvée la solution 10 modulo 41, on trouve les solutions $10^2 \equiv 18\ (mod\ 41)$, $10^3 \equiv 16\ (mod\ 41)$ et $10^4 \equiv 37\ (mod\ 41)$. L'inverse de 10 est 37 et les puissances de 37 sont une permutation des puissances de 10 : $37^2 \equiv 16\ (mod\ 41)$, $37^3 \equiv 18\ (mod\ 41)$, $37^4 \equiv 10\ (mod\ 41)$, $37^5 \equiv 1\ (mod\ 41)$.

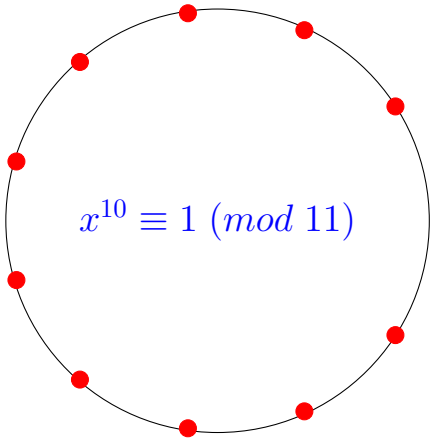
Selon un module n de dernier chiffre 9, l'équation $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) = 0\ (mod\ n)$ n'a que la solution triviale 1 car $n-1$ se terminant par un chiffre 8 ne peut être divisible par 5.

Les raisonnements ci-dessus basés sur l'étude du dernier chiffre du module s'étendent aux puissances de nombres premiers.

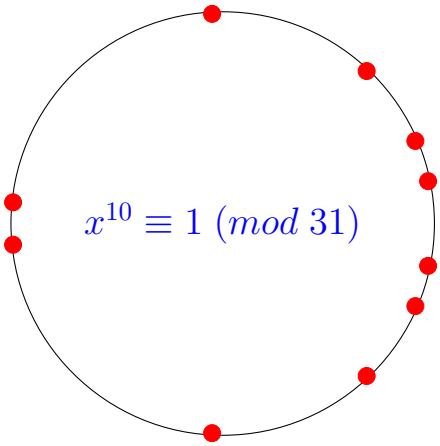
[1] Un nombre de la forme $10k$ ou $10k+5$ a pour carré un nombre $\equiv 0\ (mod\ 5)$, un nombre de la forme $10k+1$, $10k+4$, $10k+6$, $10k+9$ a pour carré un nombre $\equiv 1\ (mod\ 5)$, un nombre de la forme $10k+2$, $10k+3$, $10k+7$, $10k+8$ a pour carré un nombre $\equiv 4\ (mod\ 5)$.

Annexe 1 : Positionnement des solutions de l'équation $x^{10} \equiv 1\ (mod\ n)$ *sur cercles modulaires pour* $n = 11, 31, 41, 61, 71$ (on ne dessine pas les polygones à n côtés de sommets les n racines modulaires de l'unité, ce sont leur cosinus et sinus qui servent au positionnement des solutions).

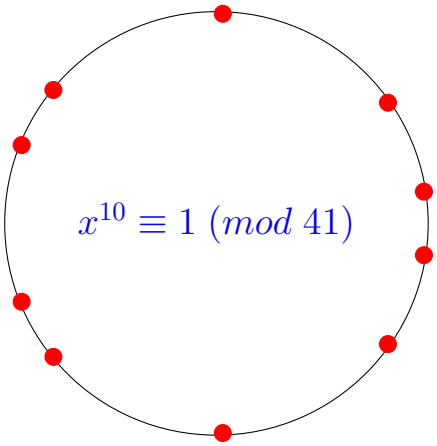
Solutions de $x^{10} \equiv 1\ (mod\ 11)$: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. 11 est premier. Il y a 10 solutions.



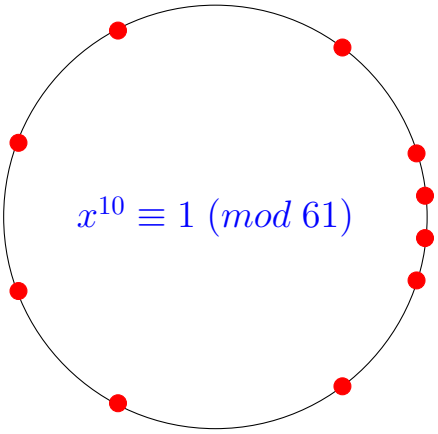
Solutions de $x^{10} \equiv 1\ (mod\ 31)$: 1, 2, 4, 8, 15, 16, 23, 27, 29, 30. 31 est premier. Il y a 10 solutions.



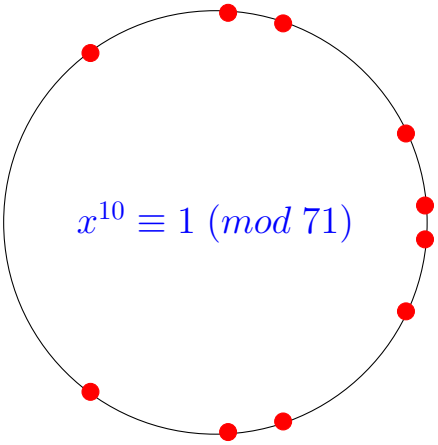
Solutions de $x^{10} \equiv 1\ (mod\ 41)$: 1, 4, 10, 16, 18, 23, 25, 31, 37, 40. 41 est premier. Il y a 10 solutions.



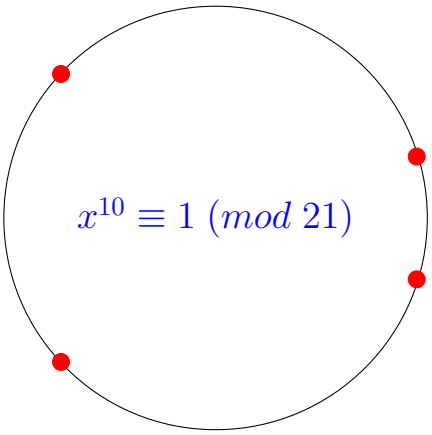
Solutions de $x^{10} \equiv 1 \ (mod\ 61)$: 1, 3, 9, 20, 27, 34, 41, 52, 58, 60. 61 est premier. Il y a 10 solutions.



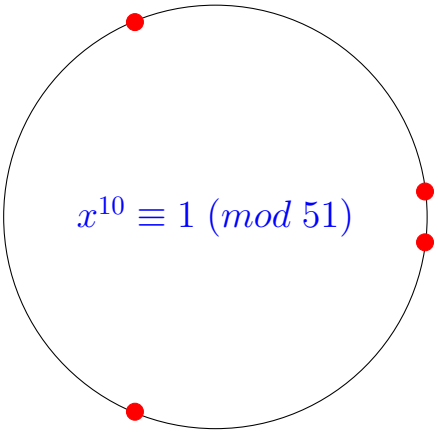
Solutions de $x^{10} \equiv 1 \ (mod\ 71)$: 1, 5, 14, 17, 25, 46, 54, 57, 66, 70. 71 est premier. Il y a 10 solutions.



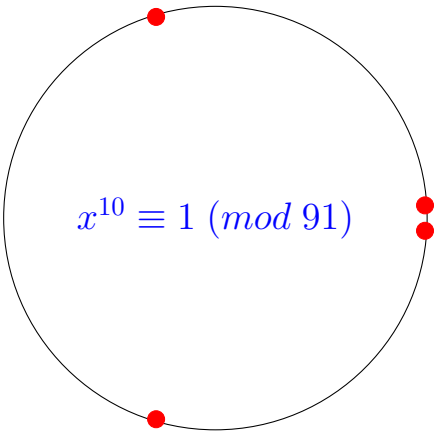
Solutions de $x^{10} \equiv 1 \ (mod\ 21)$: 1, 8, 13, 20. 21 est composé. Il y a 4 solutions.



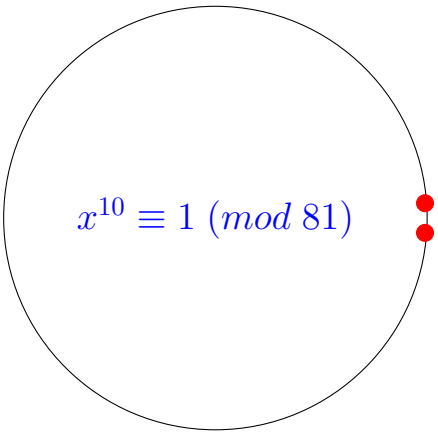
Solutions de $x^{10} \equiv 1 \ (mod\ 51)$: 1, 16, 35, 50. 51 est composé. Il y a 4 solutions.



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



Solutions de $x^{10} \equiv 1 \ (mod\ 81)$: 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 $x^{10} \equiv 1 \ (mod\ 49)$ (49 étant une puissance de 7), n'a que les deux solutions triviales 1 et 48).



Annexe 2 : Calcul des solutions de l'équation $x^4+x^3+x^2+x+1 \equiv 0\ (mod\ n)$ pour n premier de dernier chiffre 1 compris entre 31 et 100

1) modulo 31, prenons 6 qui est une des deux racines carrées de 5. La formule pour X_1 vaut :

$$\frac{\frac{-1+6}{2} \pm \sqrt{(-6)\left(\frac{1+6}{2}\right)}}{2} = \frac{\frac{3}{2} \pm \sqrt{-21}}{2}$$

Comme $-21 \equiv 196 \equiv 14^2 \equiv \left(\frac{28}{2}\right)^2\ (mod\ 11)$, on trouve comme solutions $\frac{\frac{5+28 \equiv 33 \equiv 2}{2}}{2}$ qui vaut 16 et $\frac{\frac{-23 \equiv 8}{2}}{2}$ qui vaut 2.

La formule pour X_2 amène :

$$\frac{\frac{1+6}{2} \pm \sqrt{6\left(\frac{1-6}{2}\right)}}{2}.$$

Il faut alors avoir à l'esprit que $\frac{7}{2} \equiv 19\ (mod\ 31)$ et que $\frac{6\times(-5)}{2} \equiv \frac{1}{2} \equiv 16\ (mod\ 31)$. On a alors $\frac{19 \pm 4}{2}$ qui vaut soit $\frac{15}{2} = 23$ ou $\frac{23}{2} = 27$.

2) modulo 41, prenons 13 qui est une des deux racines carrées de 5. La formule pour X_1 vaut :

$$\frac{\frac{-1+13}{2} \pm \sqrt{(-13)\left(\frac{1+13}{2}\right)}}{2} = \frac{6 \pm \sqrt{(-13)\times 7}}{2}$$

Comme $(-13)\times 7 \equiv -91 \equiv 196 \equiv 14^2\ (mod\ 41)$, on trouve comme solutions $\frac{20}{2}$ qui vaut 10 et $\frac{-8}{2}$ qui vaut -4=37.

La formule pour X_2 amène :

$$\frac{\frac{1+13}{2} \pm \sqrt{13\left(\frac{1-13}{2}\right)}}{2}.$$

$13\times(-6) \equiv -78 \equiv 4\ (mod\ 41)$. On a alors $\frac{7 \pm 2}{2}$ qui vaut soit $\frac{5}{2} = 23$ ou $\frac{9}{2} = 25$.

3) modulo 61, prenons 35 qui est une des deux racines carrées de 5. La formule pour X_1 vaut :

$$\frac{\frac{-1+35}{2} \pm \sqrt{(-35)\left(\frac{1+35}{2}\right)}}{2} = \frac{17 \pm \sqrt{(-35)\times 18}}{2}$$

Comme $(-35)\times 18 \equiv 630 \equiv 529 \equiv 23^2\ (mod\ 61)$, on trouve comme solutions $\frac{17 \pm 23}{2}$ qui vaut 20 d'une part et $-3 \equiv 58$ d'autre part.

La formule pour X_2 amène :

$$\frac{\frac{1+35}{2} \pm \sqrt{35\left(\frac{1-35}{2}\right)}}{2}.$$

$35\times(-17) \equiv -595 \equiv 625 \equiv 25^2\ (mod\ 61)$. On a alors $\frac{18 \pm 25}{2}\ (mod\ 61)$ qui vaut $\frac{43}{2} \equiv \frac{104}{2} \equiv 52\ (mod\ 61)$ ou $\frac{-7}{2} \equiv \frac{54}{2} \equiv 27\ (mod\ 61)$.

4) modulo 71, prenons 17 qui est une des deux racines carrées de 5. La formule pour X_1 vaut :

$$\frac{\frac{-1+17}{2} \pm \sqrt{(-17)\left(\frac{1+17}{2}\right)}}{2} = \frac{8 \pm \sqrt{-153}}{2}$$

Comme $-153 \equiv 841 \equiv 29^2$, on trouve comme solutions $\frac{8 \pm 29}{2}$ qui vaut $\frac{37}{2} = \frac{108}{2} = 54$ ou bien $\frac{-21}{2} = \frac{50}{2} = 25$.

La formule pour X_2 amène :

$$\frac{\frac{1+17}{2} \pm \sqrt{17\left(\frac{1-17}{2}\right)}}{2}.$$

$\frac{17 \times (-16)}{2} \equiv \frac{-272}{2} \equiv -136 \equiv 361 \equiv 19^2$ $(mod\ 71)$. On trouve comme solutions $\frac{9+19}{2} \equiv 14$ $(mod\ 71)$ et $\frac{9-19}{2} \equiv -5 \equiv 66$ $(mod\ 71)$.