$x^2 = x$

Marc Lorenzi

24 février 2026

1 L'équation

1.1 Introduction

Nous allons dans cet article résoudre l'équation « $x^2 = x$ ». Mais, me direz-vous, les solutions sont 0 et 1 ? Dans $\mathbb{R}$, certes. Mais dans $\mathbb{Z}/n\mathbb{Z}$? Soit n un entier naturel supérieur ou égal à 1. On se propose de résoudre

$$(E_n)\ x^2 = x$$

où l'inconnue x appartient à $\mathbb{Z}/n\mathbb{Z}$. Nous noterons S_n l'ensemble des solutions de (E_n).

Proposition 1.1.1. *Pour tout $n \geq 1$, $(S_n, \times)$ est un monoïde.*

Démonstration. Soit $n \geq 1$. On a $1 \in S_n$ et pour tous $x, y \in S_n$,

$$(xy)^2 = x^2y^2 = xy$$

donc $xy \in S_n$. La multiplication est donc une loi de composition interne dans S_n. Enfin, la multiplication est associative dans $\mathbb{Z}/n\mathbb{Z}$, donc aussi dans S_n. □

Remarque. Pour tout $x \in S_n$, soit $\overline{x} = 1 - x$. On a

$$\overline{x}^2 = 1 - 2x + x^2 = 1 - 2x + x = \overline{x}$$

et donc $\overline{x} \in S_n$. Or,

$$x\overline{x} = x - x^2 = 0$$

Si $x \neq 1$, alors $\overline{x} \neq 0$ et donc x est un diviseur de zéro. A fortiori, x n'est pas inversible. Le seul élément inversible de S_n est donc 1.

Remarque. Le cas $n = 1$ est un peu à part. On a dans ce cas $0 = 1$ et $S_1 = \{0\}$.

1.2 Nombres premiers

Proposition 1.2.1. *Soit n un entier naturel premier. On a $S_n = \{0, 1\}$.*

Démonstration. Comme n est premier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps. Pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, $x^2 = x$ si et seulement si $x(x-1) = 0$. Comme un corps est un anneau intègre, ceci équivaut à $x = 0$ ou $x = 1$. □

Proposition 1.2.2. *Soient p un entier naturel premier et $k \in \mathbb{N}^*$. On a $S_{p^k} = \{0, 1\}$.*

Démonstration. Montrons par récurrence sur k que pour tout $k \geq 1$, pour tout $x \in \mathbb{Z}$, si $x^2 \equiv x \bmod p^k$, alors $x \equiv 0 \bmod p^k$ ou $x \equiv 1 \bmod p^k$. Ceci prouvera que $S_{p^k} \subseteq \{0, 1\}$, l'autre inclusion étant évidente.

Nous avons déjà prouvé le résultat pour $k = 1$. Soit $k \geq 2$. Supposons que pour tout $x \in \mathbb{Z}$, si $x^2 \equiv x \bmod p^{k-1}$, alors $x \equiv 0 \bmod p^{k-1}$ ou $x \equiv 1 \bmod p^{k-1}$.

Soit $x \in \mathbb{Z}$. Supposons $x^2 \equiv x \bmod p^k$. On a donc a fortiori $x^2 \equiv x \bmod p^{k-1}$. Par l'hypothèse de récurrence, $x \equiv 0 \bmod p^{k-1}$ ou $x \equiv 1 \bmod p^{k-1}$.

- Cas 1, $x \equiv 0 \bmod p^{k-1}$. Posons $x = p^{k-1}y$ où $y \in \mathbb{Z}$. On a

  $$p^{2k-2}y^2 \equiv p^{k-1}y \bmod p^k$$

  et donc

  $$p^{k-1}y^2 \equiv y \bmod p$$

  Comme $k \geq 2$, on a

  $$p^{k-1} \equiv 0 \bmod p$$

  et donc $y \equiv 0 \bmod p$. De là, $x = p^{k-1}y \equiv 0 \bmod p^k$.
- Cas 2, $x \equiv 1 \bmod p^{k-1}$. Posons $x = 1 + p^{k-1}y$ où $y \in \mathbb{Z}$. On a

  $$(1 + p^{k-1}y)^2 \equiv 1 + p^{k-1}y \bmod p^k$$

  ou encore, en développant,

  $$2p^{k-1}y + p^{2k-2}y^2 \equiv p^{k-1}y \bmod p^k$$

  En simplifiant par p^{k-1}, il vient

  $$2y + p^{k-1}y^2 \equiv y \bmod p$$

  d'où, comme $k \geq 2$,

  $$y \equiv -p^{k-1}y^2 \equiv 0 \bmod p$$

  De là, $x = 1 + p^{k-1}y \equiv 1 \bmod p^k$.

□

1.3 Quelques valeurs

Jusqu'à présent, les résultats obtenus sont décevants. Nous aurions aimé trouver des nombres magiques égaux à leur carré, mais nous n'avons toujours que 0 et 1. Rassurons nous : si n n'est pas une puissance d'un nombre premier, la situation devient beaucoup plus intéressante. Voici l'ensemble S_n pour quelques valeurs de n.

n	S_n
6	$0, 1, 3, 4$
10	$0, 1, 5, 6$
12	$0, 1, 4, 9$
14	$0, 1, 7, 8$
15	$0, 1, 6, 10$
18	$0, 1, 9, 10$
20	$0, 1, 5, 16$

Pour de plus grandes valeurs de n, l'équation (E_n) peut avoir beaucoup de solutions. Par exemple,

$$\begin{aligned} S_{2310} \quad = \quad & \{0, 1, 210, 231, 330, 385, 441, 540, 561, 595, 616, 715, 771, 826, \\ & 925, 946, 1155, 1156, 1365, 1386, 1485, 1540, 1596, 1695, 1716, \\ & 1750, 1771, 1870, 1926, 1981, 2080, 2101\} \end{aligned}$$

On a $2310 = 2 \times 3 \times 5 \times 7 \times 11$. L'ensemble S_{2310} est de cardinal 32.

1.4 Produits d'entiers premiers entre eux

Donnons nous deux entiers naturels a et b non nuls. Supposons que $\text{pgcd}(a, b) = 1$.

Remarquons que si $x, y \in \mathbb{Z}$ vérifient $x \equiv y \bmod ab$, alors $x \equiv y \bmod a$ et $x \equiv y \bmod b$. On définit donc bien une application $\varphi : \mathbb{Z}/ab\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ en posant pour tout $x \in \mathbb{Z}$,

$$\varphi(x + ab\mathbb{Z}) = (x + a\mathbb{Z}, x + b\mathbb{Z})$$

Proposition 1.4.1. *φ est un isomorphisme d'anneaux.*

Démonstration. On munit évidemment $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ de la structure d'anneau produit. Les propriétés de morphisme sont de simples vérifications. Soit $x \in \mathbb{Z}$. Supposons que $x+ab\mathbb{Z} \in \ker \varphi$. On a $x \equiv 0 \bmod a$ et $x \equiv 0 \bmod b$ donc, comme a et b sont premiers entre eux, $x \equiv 0 \bmod ab$. Ainsi, $\ker \varphi = \{0\}$, d'où l'injectivité de φ. Il reste à remarquer que les ensembles de départ et d'arrivée de φ ont le même cardinal, puisque

$$ab = |\mathbb{Z}/ab\mathbb{Z}| = |\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}|$$

où les barres verticales désignent le cardinal des ensembles. Ainsi, φ est bijectif. □

Proposition 1.4.2. $\varphi(S_{ab}) = S_a \times S_b$.

Démonstration. Soit $x \in \mathbb{Z}$. On a $x + ab\mathbb{Z} \in S_{ab}$ si et seulement si $x^2 - x \equiv 0 \bmod ab$. Comme a et b sont premiers entre eux, ceci équivaut à $x^2 - x \equiv 0 \bmod a$ et $x^2 - x \equiv 0 \bmod b$, c'est à dire $x + a\mathbb{Z} \in S_a$ et $x + b\mathbb{Z} \in S_b$, ou encore $\varphi(x + ab\mathbb{Z}) \in S_a \times S_b$. □

Corollaire 1.4.3. $|S_{ab}| = |S_a| \times |S_b|$.

Démonstration. L'application φ est injective, donc elle conserve les cardinaux. □

Il est facile d'étendre ce résultat à plus de deux entiers.

Proposition 1.4.4. *Soit $r \geq 1$. Soient $a_1, \ldots, a_r \in \mathbb{N}^*$. On suppose les a_i premiers entre eux deux à deux. On a alors*

$$|S_{a_1 \ldots a_r}| = \prod_{i=1}^{r} |S_{a_i}|$$

Démonstration. On procède par récurrence sur r. Pour $r = 1$ il n'y a rien à prouver. Soit $r \geq 2$. Supposons la propriété vérifiée par $r-1$. Soient $a_1, \ldots, a_r \in \mathbb{N}^*$. Supposons les a_i premiers entre eux deux à deux. Les entiers $a_1 \ldots a_{r-1}$ et a_r sont alors premiers entre eux. Par le corollaire précédent,

$$|S_{a_1 \ldots a_r}| = |S_{a_1 \ldots a_{r-1}}| \times |S_{a_r}|$$

On termine en utilisant l'hypothèse de récurrence. □

1.5 Le nombre de solutions

Proposition 1.5.1. *Soit $n \in \mathbb{N}^*$. Le cardinal de S_n est 2^r où r est le nombre de diviseurs premiers de n.*

Démonstration. Le cas $n = 1$ est immédiat. Supposons donc $n \geq 2$, et donc $r \geq 1$. Écrivons

$$n = \prod_{k=1}^{r} p_k^{\alpha_k}$$

où les p_k sont les diviseurs premiers distincts de n et les α_k des entiers naturels non nuls. Les $p_k^{\alpha_k}$ sont premiers entre eux deux à deux donc, par la proposition 1.4.4,

$$|S_n| = \prod_{k=1}^{r} |S_{p_k^{\alpha_k}}|$$

Par la proposition 1.2.2, on a pour tout $k \in [\![1, r]\!]$,

$$|S_{p_k^{\alpha_k}}| = 2$$

d'où le résultat. □

2 Le calcul effectif des solutions

Nous savons maintenant *combien* l'équation (E_n) possède de solutions. Il nous reste à savoir comment les calculer. Une solution naïve consiste évidemment à passer en revue tous les entiers entre 0 et $n-1$. Si n est grand, ceci ne peut pas être fait en un temps raisonnable.

2.1 Le théorème des restes chinois

Soit $n \in \mathbb{N}^*$. Supposons connue la décomposition de n en produit de nombres premiers. Ce qui précède montre que pour déterminer S_n, il suffit de savoir faire la chose suivante : si $a, b \in \mathbb{N}^*$ sont premiers entre eux et que l'on connaît S_a et S_b, déterminer S_{ab}.

Rappelons l'isomorphisme $\varphi : \mathbb{Z}/ab\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. On a

$$S_{ab} = \varphi^{-1}(S_a \times S_b)$$

Le calcul explicite de φ^{-1} est classique : il s'agit du *théorème des restes chinois*. Soient $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$. Soient $y, z \in \mathbb{Z}$ tels que $y + a\mathbb{Z} \in S_a$ et $z + b\mathbb{Z} \in S_b$. Soit $x = uaz + vby$. On a

$$x \equiv vby \equiv (1 - ua)y \equiv y \bmod a$$

et de même

$$x \equiv z \bmod b$$

Ainsi,

$$\varphi^{-1}(y + a\mathbb{Z}, z + b\mathbb{Z}) = x + ab\mathbb{Z}$$

De façon plus explicite,

$$S_{ab} = \{uaz + vby + ab\mathbb{Z} : y + a\mathbb{Z} \in S_a, z + b\mathbb{Z} \in S_b\}$$

Supposons que $n = p_1^{k_1} \dots p_r^{k_r}$ où les p_i sont des nombres premiers distincts et les k_i des entiers non nuls. Sachant que $S_1 = \{0\}$, une simple boucle suffit pour calculer successivement les ensembles $S_{p_1^{k_1} \dots p_j^{k_j}}$ pour $j \in [\![1, r]\!]$. On obtient ainsi S_n en r itérations.

2.2 Deux exemples

Exemple 1. Prenons pour n une puissance de 10. Dans ce cas, n possède deux diviseurs premiers (2 et 5) donc S_n est de cardinal 4. Cet ensemble contient 0, 1 et deux autres éléments α et β. Rappelons nous que $1 - \alpha \in S_n$, donc $\beta = 1 - \alpha$. Voici α et β pour $n = 10^{75}$.

$$\begin{aligned} \alpha &= 1099378334904191361889994425765767691038909958933800226077437400817871093 76 \\ \beta &= 8900621665095808638110005574234232308961090041066199773922562599182128906 25 \end{aligned}$$

Ces deux nombres magiques vérifient $\alpha^2 = \alpha$, $\beta^2 = \beta$, $\alpha + \beta = 1$ et $\alpha\beta = 0$.

Exemple 2. Prenons un entier n qui a « beaucoup » de diviseurs premiers. La page suivante liste les éléments de l'ensemble S_n pour $n = 19! = 121645100408832000$. L'entier n possède 8 diviseurs premiers qui sont 2, 3, 5, 7, 11, 13, 17 et 19. L'ensemble S_n est donc de cardinal $2^8 = 256$. Une recherche naïve des solutions de (E_n) aurait été impossible. En utilisant le théorème des restes chinois, on obtient instantanément les solutions.

0	1	610877575397376	1307364953882625	1489744252698625
1898852917248001	2402898960384000	2585278259200000	3817095446528001	3892643213082625
3999474745344001	4400749555941376	4503520788480000	5791496130330625	6402373705728001
7709738659610625	7872897794048001	7892117958426625	8055277092864001	8293392769024000
9973519622144001	10295016918810625	10803123261669376	11765541007130625	11822274064613376
11947920305946625	13866162835226625	14275271499776001	14457650798592001	14695766474752000
14858925609189376	15714917277696000	16375893327872001	16777168138469376	16959547437285376
17613770194944001	18167914712858625	18224647770341376	18350294011674625	18751568822272000
19532012724224001	19714392023040001	20268536540954625	20669811351552000	20852190650368000
21261299314917376	21506413408026625	22117290983424000	23179541844197376	23361921143013376
23424655937306625	23607035236122625	24016143900672001	25153942528000000	25934386429952001
26116765728768001	26518040539365376	27072185057280000	27254564356096000	27587289817088001
27908787113754625	29827029643034625	29990188777472001	30009408941850625	30172568076288001
30410683752448000	31479933030170625	32090810605568001	32920414245093376	33882831990554625
33989663522816001	34065211289370625	34390938333413376	34573317632229376	35983453818650625
36392562483200001	36491560161509376	36574941782016001	36813057458176000	36976216592613376
37882306735898625	38283581546496000	38465960845312000	38493184311296001	38894459121893376
39076838420709376	40285205696282625	40384203374592000	40467584995098625	40793312039141376
40868859805696000	40975691337957376	42283056291840001	42385827524378625	42787102334976000
42893933867237376	42969481633792000	43378590298341376	44685955252224000	44868334551040000
45296832827621376	45479212126437376	46175699504922625	46786577080320000	46949736214757376
47271233511424000	48685429997568001	49189476040704000	49371855339520000	49704580800512001
50842379427840000	52578073210650625	52741232345088001	53352109920485376	53597224013594625
54659474874368001	54841854173184001	56106954506240001	56508229316837376	56633875558170625
56690608615653376	57244753133568000	58552118087450625	58608851144933376	58734497386266625
59143606050816001	59999597719322625	60400872529920000	60583251828736000	61061848580096001
61244227878912001	61645502689509376	62501494358016000	62910603022565376	63036249263898625
63092982321381376	64400347275264001	64954491793178625	65011224850661376	65136871091994625
65538145902592000	66803246235648000	66985625534464000	68047876395237376	68292990488346625
68903868063744000	69067027198181376	70802720980992001	71940519608320000	72273245069312001
72455624368128001	72959670411264000	74373866897408001	74695364194074625	74858523328512001
75469400903909376	76165888282394625	76348267581210625	76776765857792001	76959145156608001
78266510110490625	78675618775040001	78751166541594625	78857998073856001	79259272884453376
79362044116992000	80669409070874625	80776240603136001	80851788369690625	81177515413733376
81260897034240001	81359894712549376	82568261988122625	82750641286938625	83151916097536000
83179139563520001	83361518862336001	83762793672933376	84668883816218625	84832042950656001
85070158626816000	85153540247322625	85252537925632000	85661646590181376	87071782776602625
87254162075418625	87579889119461376	87655436886016000	87762268418277376	88724686163738625
89554289803264000	90165167378661376	91234416656384001	91472532332544000	91635691466981376
91654911631360000	91818070765797376	93736313295077376	94057810591744000	94390536052736001
94572915351552001	95127059869466625	95528334680064000	95710713978880000	96491157880832001
97628956508160000	98038065172709376	98220444471525376	98283179265818625	98465558564634625
99527809425408001	100138687000805376	100383801093914625	100792909758464001	100975289057280001
101376563867877376	101930708385792000	102113087684608000	102893531586560001	103294806397157376
103420452638490625	103477185695973376	104031330213888000	104685552971546625	104867932270362625
105269207080960000	105930183131136001	106786174799642625	106949333934080001	107187449610240000
107369828909056000	107778937573605376	109697180102885376	109822826344218625	109879559401701376
110841977147162625	111350083490021376	111671580786688000	113351707639808001	113589823315968000
113752982450405376	113772202614784000	113935361749221376	115242726703104000	115853604278501376
117141579620352001	117244350852890625	117645625663488000	117752457195749376	117828004962304000
119059822149632001	119242201448448001	119746247491584000	120155356156133376	120377735454949376
121034222833434625				

3 Le code Python

La fonction `solve` ci dessous a été utilisée pour calculer les valeurs données dans les exemples. Elle prend en paramètre un entier naturel n non nul. Elle renvoie la liste des éléments de S_n, ou plus exactement des représentants de ces éléments qui appartiennent à l'intervalle $[\![0, n-1]\!]$. La liste renvoyée est triée dans l'ordre croissant.

Cette fonction appelle deux fonctions auxiliaires dont je ne donnerai pas le code :

- La fonction `facteurs` prend en paramètre un entier naturel non nul n. Elle renvoie la liste des couples (p, k) où p décrit l'ensemble des diviseurs premiers de n et k est la valuation p-adique de n.
- La fonction `ext_gcd` prend en paramètres deux entiers relatifs a et b. Elle renvoie un triplet (u, v, d) d'entiers tel que $ua + vb = d$ et d est le pgcd positif de a et b.

```
def solve(n):
    fs = facteurs(n)
    S = [0]
    a = 1
    for p, k in fs:
        b = p ** k
        u, v, _ = ext_gcd(a, b)
        S1 = []
        for y in S:
            for z in [0, 1]:
                x = (u * a * z + v * b * y) % (a * b)
                S1.append(x)
        a = a * b
        S = S1
    S.sort()
    return S
```