$x^2 = -1$

Marc Lorenzi

28 février 2026

1 Résidus quadratiques

1.1 Introduction

Pour tout entier $n \geq 1$, $\mathbb{Z}_n$ est l'ensemble des entiers modulo n. La notation usuelle est plutôt $\mathbb{Z}/n\mathbb{Z}$, mais $\mathbb{Z}_n$ est plus concis. Muni de l'addition et de la multiplication, $\mathbb{Z}_n$ est un anneau commutatif. Nous noterons $\mathbb{Z}_n^\times$ le groupe des inversibles de $\mathbb{Z}_n$. Pour tout $x \in \mathbb{Z}$, la classe de x modulo n est $x + n\mathbb{Z}$. On a

$$\mathbb{Z}_n^\times = \{x + n\mathbb{Z} : x \in \mathbb{Z}, \text{pgcd}(x, n) = 1\}$$

Si n est premier, alors $\mathbb{Z}_n$ est un corps et donc $\mathbb{Z}_n^\times = \mathbb{Z}_n \setminus \{0\}$. Si, au contraire, n est composé, alors l'anneau $\mathbb{Z}_n$ n'est pas intègre.

Lorsque n est composé, un polynôme de degré 2 à coefficients dans $\mathbb{Z}_n$ peut avoir plus de deux racines. Le polynôme auquel nous allons nous intéresser dans cet article est $X^2 + 1$. Selon les valeurs de n, combien ce polynôme a-t-il de racines dans $\mathbb{Z}_n$? Comment calculer efficacement ces racines ?

1.2 Résidus quadratiques

Soit $n \geq 1$. Notons $\mathcal{R}_n$ l'ensemble des carrés des éléments de $\mathbb{Z}_n^\times$:

$$\mathcal{R}_n = \{x^2 : x \in \mathbb{Z}_n^\times\}$$

Les éléments de $\mathcal{R}_n$ sont les *résidus quadratiques* modulo n. Voici, pour $n \leq 15$, les éléments de l'ensemble $\mathcal{R}_n$.

n	$\mathcal{R}_n$
1	0
2	1
3	1
4	1
5	1, 4
6	1
7	1, 2, 4
8	1
9	1, 4, 7
10	1, 9
11	1, 3, 4, 5, 9
12	1
13	1, 3, 4, 9, 10, 12
14	1, 9, 11
15	1, 4

Proposition 1. *$\mathcal{R}_n$ est un sous-groupe de $\mathbb{Z}_n^\times$.*

Démonstration. On a $1 = 1^2$ donc $1 \in \mathcal{R}_n$. Soient $x, y \in \mathcal{R}_n$. Il existe $a, b \in \mathbb{Z}_n^\times$ tels que $x = a^2$ et $y = b^2$. On a alors

$$xy^{-1} = (ab^{-1})^2 \in \mathcal{R}_n$$

□

Proposition 2. *Soit p un nombre premier impair. Pour tout $x \in \mathbb{Z}_p^\times$, $x^{(p-1)/2} = \pm 1$.*

Démonstration. Soit $x \in \mathbb{Z}_p^\times$. Par le petit théorème de Fermat, $x^{p-1} = 1$. En posant $y = x^{(p-1)/2}$, on a donc $y^2 = 1$, ou encore $(y-1)(y+1) = 0$. Comme p est premier, $\mathbb{Z}_p$ est un anneau intègre et donc $y = \pm 1$. □

Que se passe-t-il si p n'est pas premier ? Si p est pair, l'égalité de la proposition n'a pas de sens, puisque $(p-1)/2$ n'est pas entier. Si p est impair, le résultat est en général faux. Par exemple si $p = 15$, on a $(p-1)/2 = 7$. Pourtant, $4^7 = 4 \neq \pm 1$ alors que $4 \in \mathbb{Z}_{15}^\times$.

Proposition 3. *Soit p un nombre premier impair. Le cardinal de $\mathcal{R}_p$ est $(p-1)/2$.*

Démonstration. Considérons l'application $\varphi : \mathbb{Z}_p^\times \longrightarrow \mathcal{R}_p$ définie par $\varphi(x) = x^2$. Cette application est surjective. Soient $x, y \in \mathbb{Z}_p^\times$. On a $\varphi(x) = \varphi(y)$ si et seulement si $x^2 = y^2$, ou encore $(x-y)(x+y) = 0$, c'est à dire $y = \pm x$. Comme p est impair, $-x \neq x$. Les éléments de $\mathcal{R}_p$ ont donc chacun exactement 2 antécédents par φ. Par le lemme des bergers,

$$|\mathbb{Z}_p^\times| = 2|\mathcal{R}_p|$$

d'où le résultat. □

Proposition 4. *Soit p un nombre premier impair. Soit $x \in \mathbb{Z}_p^\times$. On a*

$$\begin{aligned} x \in \mathcal{R}_p &\iff x^{(p-1)/2} = 1 \\ x \in \mathbb{Z}_p^\times \setminus \mathcal{R}_p &\iff x^{(p-1)/2} = -1 \end{aligned}$$

Démonstration. Considérons le polynôme

$$P = X^{(p-1)/2} - 1 \in \mathbb{Z}_p[X]$$

Soit $x \in \mathcal{R}_p$. Soit $a \in \mathbb{Z}_p^\times$ tel que $x = a^2$. Par le petit théorème de Fermat,

$$P(x) = a^{p-1} - 1 = 0$$

et donc x est racine de P. Les éléments de $\mathcal{R}_p$ sont donc *des* racines de P. Or, P est de degré $(p-1)/2$. Le polynôme P a donc au plus $(p-1)/2$ racines. Comme $\mathcal{R}_p$ est de cardinal $(p-1)/2$, *les* racines de P sont *les* éléments de R_p.

Soit $x \in \mathbb{Z}_p^\times$. On a $x \in \mathbb{Z}_p^\times \setminus \mathcal{R}_p$ si et seulement si $x^{(p-1)/2} \neq 1$. Par la proposition 2, ceci équivaut à $x^{(p-1)/2} = -1$. □

Remarque. Soient p un nombre premier impair. Comme $\mathcal{R}_p$ est un sous-groupe de $\mathbb{Z}_p^\times$, on a

- Pour tous $x, y \in \mathcal{R}_p$, $xy \in \mathcal{R}_p$.
- Pour tout $x \in \mathcal{R}_p$ et tout $y \in \mathbb{Z}_p^\times \setminus \mathcal{R}_p$, $xy \in \mathbb{Z}_p^\times \setminus \mathcal{R}_p$.

On peut ici dire un peu mieux. Pour tous $x, y \in \mathbb{Z}_p^\times \setminus \mathcal{R}_p$,

$$(xy)^{(p-1)/2} = x^{(p-1)/2} y^{(p-1)/2} = (-1)^2 = 1$$

et donc $xy \in \mathcal{R}_p$.

1.3 Un cas particulier

Proposition 5. *Soit p un nombre premier impair. On a $-1 \in \mathcal{R}_p$ si et seulement si $p \equiv 1 \bmod 4$.*

Démonstration. Par la proposition 4, $-1 \in \mathcal{R}_p$ si et seulement si $(-1)^{(p-1)/2} = 1$, c'est à dire $(p-1)/2$ est pair, ou encore $p-1$ est multiple de 4. □

Voici, pour les nombres premiers p congrus à 1 modulo 4 et inférieurs ou égaux à 101, les racines carrées r de -1 dans $\mathbb{Z}_p$. Ces deux racines sont évidemment opposées. Pour de petits entiers p, ces racines peuvent être obtenues par une méthode naïve, en considérant un après l'autre tous les éléments de $\mathbb{Z}_p^\times$. Nous verrons plus loin qu'on peut faire bien mieux que cela.

p	5	13	17	29	37	41	53	61	73	89	97	101
r	$2, 3$	$5, 8$	$4, 13$	$12, 17$	$6, 31$	$9, 32$	$23, 30$	$11, 50$	$27, 46$	$34, 55$	$22, 75$	$10, 91$

1.4 Digression

Existe-t-il beaucoup de nombres premiers congru à 1 modulo 4 ? Congrus à 3 modulo 4 ? Oui. Dans les deux cas il y en a une infinité.

Proposition 6. *Il existe une infinité de nombres premiers congrus à 3 modulo 4.*

La preuve suit la preuve classique utilisée pour montrer qu'il existe une infinité de nombres premiers.

Démonstration. Supposons que l'ensemble E des nombres premiers congrus à 3 modulo 4 est fini. Soit

$$n = 4 \prod_{p \in E, p \neq 3} p + 3$$

L'entier n n'est divisible par aucun élément de E. De plus, n n'est divisible ni par 2 ni par 3, donc tous les diviseurs premiers de n sont congrus à 1 modulo 4. Écrivons

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

où les p_k sont les diviseurs premiers de n (tous congrus à 1 modulo 4) et les α_k sont des entiers non nuls. Chacun des facteurs du produit est congru à 1 modulo 4, donc $n \equiv 1 \bmod 4$. Contradiction. □

Proposition 7. *Il existe une infinité de nombres premiers congrus à 1 modulo 4.*

Cette propriété est moins élémentaire que la précédente.

Démonstration. Soit E l'ensemble des nombres premiers congrus à 1 modulo 4. Soit $n > 1$. Nous allons montrer qu'il existe un élément de E strictement supérieur à n. Soit p le plus petit diviseur premier de $N = n!^2 + 1$. On a $n!^2 \equiv -1 \bmod p$, donc $-1 \in \mathcal{R}_p$. Par la proposition 5, $p \equiv 1 \bmod 4$. De plus, aucun entier inférieur ou égal à n ne divise N, donc $p > n$. □

Ces deux résultats sont des cas particuliers d'un théorème beaucoup plus général, le *théorème de la progression arithmétique de Dirichlet* : si a et b sont deux entiers naturels non nuls premiers entre eux, il existe une infinité de nombres premiers de la forme $an + b$, où $n \in \mathbb{N}$.

2 Une équation du second degré

2.1 Introduction

Pour tout $n \in \mathbb{N}^*$, considérons l'équation

$$(E_n)\ x^2 = -1$$

d'inconnue $x \in \mathbb{Z}_n$. Nous noterons $\mathcal{S}_n$ l'ensemble des solutions de (E_n). Nous allons procéder par étapes. Tout d'abord, le cas où n est une puissance de 2. Puis le cas où n est une puissance d'un nombre premier impair. Enfin, le cas général.

Remarque. Le cas $n = 1$ est un peu à part. On a $\mathcal{S}_1 = \{0\}$ (ou $\{1\}$, si l'on préfère, puisque dans $\mathbb{Z}_1$, $0 = 1$).

2.2 Les puissances de 2

Le cas des puissances de 2 est facile à traiter.

Proposition 8. *On a $\mathcal{S}_2 = \{1\}$ et pour tout $k \geq 2$, $\mathcal{S}_{2^k} = \emptyset$.*

Démonstration. Dans $\mathbb{Z}_2$, $(-1)^2 = 1 = -1$ donc $\mathcal{S}_2 = \{1\}$. Soit $k \geq 2$. Soit $x \in \mathbb{Z}$. Supposons $x^2 + 1 \equiv 0 \bmod 2^k$. A fortiori, $x^2 + 1 \equiv 0 \bmod 4$, ou encore $x^2 \equiv 3 \bmod 4$. Or, les seuls carrés modulo 4 sont 0 et 1. □

2.3 Les nombres premiers impairs et leurs puissances

Proposition 9. *Soit p un nombre premier impair. Si $p \equiv 3 \mod 4$, alors $\mathcal{S}_p = \emptyset$. Sinon, $\mathcal{S}_p$ est de cardinal 2.*

Démonstration. Par la proposition 5, $-1 \in \mathcal{R}_p$ si et seulement si $p \equiv 1 \bmod 4$. Donc, si $p \equiv 3 \bmod 4$, alors $\mathcal{S}_p = \emptyset$.

Supposons maintenant $p \equiv 1 \bmod 4$. Par la proposition 5, $-1 \in \mathcal{R}_p$ et donc $\mathcal{S}_p \neq \emptyset$. Soit $a \in \mathcal{S}_p$. Pour tout $x \in \mathbb{Z}_p^\times$, $x \in \mathcal{S}_p$ si et seulement si $x^2 = a^2$, c'est à dire

$$(x - a)(x + a) = 0$$

Comme $\mathbb{Z}_p$ est un corps, on a donc $x \in \mathcal{S}_p$ si et seulement si $x = \pm a$. Enfin, comme p est impair, $a \neq -a$. L'ensemble $\mathcal{S}_p$ est donc de cardinal 2. □

Proposition 10. *Soient p un nombre premier impair et $k \geq 1$. Si $p \equiv 3 \mod 4$, alors $\mathcal{S}_{p^k} = \emptyset$. Sinon, $\mathcal{S}_{p^k}$ est de cardinal 2.*

Démonstration. Soit $x \in \mathbb{Z}$. Si $x^2 + 1 \equiv 0 \bmod p^k$, alors $x^2 + 1 \equiv 0 \mod p$. Dit autrement, si $x + p^k\mathbb{Z} \in \mathcal{S}_{p^k}$, alors $x + p\mathbb{Z} \in \mathcal{S}_p$. Si $p \equiv 3 \bmod 4$, alors $\mathcal{S}_p = \emptyset$, donc on a aussi $\mathcal{S}_{p^k} = \emptyset$.

Supposons maintenant $p \equiv 1 \bmod 4$. Supposons que $\mathcal{S}_{p^k}$ possède un élément a. On a alors $(-a)^2 = a^2 = -1$, donc $-a \in \mathcal{S}_{p^k}$. Comme p est impair, $-a \neq a$. On a donc $\{-a, a\} \subseteq \mathcal{S}_{p^k}$. In versement, soit $x \in \mathbb{Z}$. Supposons que $x^2 + 1 \equiv 0 \bmod p^k$. On a donc

$$(\star)\ (x - a)(x + a) \equiv 0 \bmod p^k$$

Supposons que p divise $x-a$. Supposons que p divise aussi $x+a$. Alors, p divise $(x+a)-(x-a) = 2a$. Or, p est impair, donc p divise a. Mais $a^2 \equiv -1 \bmod p$, contradiction. De là, comme p ne divise pas $x + a$, $x + a$ est inversible modulo p^k. En multipliant $(\star)$ par l'inverse de $x + a$, on obtient $x - a \equiv 0 \bmod p^k$ et donc $x + p^k\mathbb{Z} = a$.

Si, au contraire, p ne divise pas $x-a$, alors $x-a$ est inversible modulo p^k et le même raisonnement nous dit que $x + p^k\mathbb{Z} = -a + p^k\mathbb{Z}$. Ainsi, si $\mathcal{S}_{p^k} \neq \emptyset$, alors cet ensemble est de cardinal 2.

Montrons maintenant par récurrence sur k que pour tout $k \geq 1$, $\mathcal{S}_{p^k} \neq \emptyset$. Nous avons déjà le résultat si $k = 1$. Soit $k \geq 2$. Supposons que $\mathcal{S}_{p^{k-1}} \neq \emptyset$. Soit $x \in \mathbb{Z}$ tel que $x^2 + 1 \equiv 0 \bmod p^{k-1}$. Posons $x^2 = -1 + p^{k-1}u$, où $u \in \mathbb{Z}$. Soit

$$y = x + vp^{k-1}$$

où $v \in \mathbb{Z}$. On a

$$\begin{aligned} y^2 + 1 &= x^2 + v^2p^{2k-2} + 2vxp^{k-1} + 1 \\ &= v^2p^{2k-2} + (2vx + u)p^{k-1} \\ &\equiv (2vx + u)p^{k-1} \bmod p^k \end{aligned}$$

car $k \geq 2$ et donc $2k - 2 \geq k$. De là, $y^2 + 1 \equiv 0 \bmod p^k$ si et seulement si

$$(\star)\ 2vx + u \equiv 0 \bmod p$$

Remarquons que comme $x^2 \equiv -1 \bmod p$ et p est premier impair, $2x$ est inversible modulo p. Il existe donc, modulo p, un (unique) u vérifiant $(\star)$. L'ensemble $\mathcal{S}_{p^k}$ est donc non vide. □

2.4 Entiers premiers entre eux

Soient a et b deux entiers naturels non nuls premiers entre eux.

Pour tous $x, y \in \mathbb{Z}$, si $x + ab\mathbb{Z} = y + ab\mathbb{Z}$, alors $x + a\mathbb{Z} = y + a\mathbb{Z}$ et $x + b\mathbb{Z} = y + b\mathbb{Z}$. On définit donc une fonction $\varphi : \mathbb{Z}_{ab} \longrightarrow \mathbb{Z}_a \times \mathbb{Z}_b$ en posant, pour tout $x \in \mathbb{Z}$,

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

Proposition 11. *φ est un isomorphisme d'anneaux.*

Démonstration. Les propriétés de morphisme sont immédiates à vérifier. Montrons que φ est injectif. Soit $x \in \mathbb{Z}$. Supposons $\varphi(x + ab\mathbb{Z}) = 0$. On a $x + a\mathbb{Z} = 0$ et $x + b\mathbb{Z} = 0$, c'est à dire $x \in a\mathbb{Z} \cap b\mathbb{Z}$. Comme a et b sont premiers entre eux, $a\mathbb{Z} \cap b\mathbb{Z} = ab\mathbb{Z}$. Ainsi, $x \in ab\mathbb{Z}$ donc $x + ab\mathbb{Z} = ab\mathbb{Z}$. On en déduit que $\ker \varphi = \{0\}$. Le morphisme φ est donc injectif. Remarquons pour terminer que

$$ab = |\mathbb{Z}_{ab}| = |\mathbb{Z}_a| \times |\mathbb{Z}_b| = |\mathbb{Z}_a \times \mathbb{Z}_b|$$

Les ensembles de départ et d'arrivée de l'injection φ sont de même cardinal, donc φ est une bijection. □

Proposition 12. *$\varphi(\mathcal{S}_{ab}) = \mathcal{S}_a \times \mathcal{S}_b$.*

Démonstration. Soit $x \in \mathbb{Z}$. Comme a et b sont premiers entre eux, $x^2 + 1 \equiv 0 \bmod ab$ si et seulement si $x^2 + 1 \equiv 0 \bmod a$ et $x^2 + 1 \equiv 0 \bmod b$. □

Proposition 13. *Soient $a, b \in \mathbb{N}^*$. On suppose a et b premiers entre eux. On a*

$$|\mathcal{S}_{ab}| = |\mathcal{S}_a| \times |\mathcal{S}_b|$$

Démonstration. On a $\varphi(\mathcal{S}_{ab}) = \mathcal{S}_a \times \mathcal{S}_b$. Comme φ est injectif, φ conserve les cardinaux. On a donc

$$|\mathcal{S}_{ab}| = |\mathcal{S}_a \times \mathcal{S}_b| = |\mathcal{S}_a| \times |\mathcal{S}_b|$$

□

Ce résultat se généralise sans difficulté à un nombre quelconque d'entiers.

Proposition 14. *Soit $r \geq 1$. Soient $a_1, \ldots, a_r \in \mathbb{N}^*$ premiers entre eux deux à deux. On a*

$$|\mathcal{S}_{a_1 \ldots a_r}| = \prod_{i=1}^{r} |\mathcal{S}_{a_i}|$$

Démonstration. On procède par récurrence sur r. Si $r = 1$, il n'y a rien à montrer. Soit $r \geq 2$. Supposons la propriété vérifiée par $r-1$. Soient $a_1, \ldots, a_r \in \mathbb{N}^*$ premiers entre eux deux à deux. Les deux entiers $a_1 \ldots a_{r-1}$ et a_r sont premiers entre eux donc, par la proposition 13,

$$|\mathcal{S}_{a_1 \ldots a_r}| = |\mathcal{S}_{a_1 \ldots a_{r-1}}| \times |\mathcal{S}_{a_r}|$$

On termine grâce à l'hypothèse de récurrence. □

2.5 Le cas général

Nous pouvons maintenant donner le résultat général. Si $n \in \mathbb{N}^*$, quel est le cardinal de $\mathcal{S}_n$?

Proposition 15. *Soit $n \in \mathbb{N}^*$. L'ensemble $\mathcal{S}_n$ est non vide si et seulement si n n'est pas un multiple de 4 et n'est divisible par aucun nombre premier congru à 3 modulo 4. Dans ce cas, le cardinal de $\mathcal{S}_n$ est 2^r où r est le nombre de diviseurs premiers de n congrus à 1 modulo 4.*

Démonstration. Supposons n multiple de 4. Supposons $\mathcal{S}_n$ non vide. Soit $x \in \mathbb{Z}$ tel que $x^2 + 1 \equiv 0 \bmod n$. On a alors a fortiori $x^2 + 1 \equiv 0 \bmod 4$. Contradiction, puisque $S_4 = \emptyset$. De même, n n'est divisible par aucun nombre premier congru à 3 modulo 4.

Supposons maintenant que n n'est pas un multiple de 4 et n'est divisible par aucun nombre premier congru à 3 modulo 4. Écrivons

$$n = 2^a \prod_{i=1}^{r} p_i^{k_i}$$

où $a = 0$ ou 1, $r \in \mathbb{N}$ et les p_i sont des nombres premiers distincts congrus à 1 modulo 4. L'entier 2 et les $p_i^{k_i}$ sont premiers entre-eux deux à deux. Par les propositions 14, 8 et 10,

$$|\mathcal{S}_n| = |\mathcal{S}_{2^a}| \prod_{i=1}^{r} \left| \mathcal{S}_{p_i^{k_i}} \right| = 1 \prod_{i=1}^{r} 2 = 2^r$$

□

3 Le calcul effectif

Nous savons *combien* l'équation (E_n) possède de solutions. Nous allons maintenant voir *comment* calculer ces solutions.

3.1 Nombres premiers impairs

Soit p un nombre premier congru à 1 modulo 4. Nous savons que -1 est un carré modulo p. Plus précisément, -1 est le carré de deux éléments opposés de $\mathbb{Z}_p^\times$. Il existe un algorithme probabiliste simple pour déterminer l'un de ces deux éléments (et donc l'autre).

Munissons $\mathbb{Z}_p^\times$ de la probabilité uniforme $\mathbb{P}$. On a $\mathbb{P}(\mathcal{R}_p) = \mathbb{P}(\mathbb{Z}_p^\times \setminus \mathcal{R}_p) = 1/2$. On commence par trouver un élément de $\mathbb{Z}_p^\times \setminus \mathcal{R}_p$. Pour cela, on tire aléatoirement un élément a de $\mathbb{Z}_p^\times$ jusqu'à obtenir ce que l'on veut. Le nombre de tirages à effectuer suit une loi géométrique de paramètre $1/2$ (et donc d'espérance et de variance égales à 2). Pour déterminer si $a \notin \mathcal{R}_p$, il suffit de calculer, par exemple par une exponentiation rapide, $a^{(p-1)/2}$. Ce calcul s'effectue en $O(\log p)$ opérations sur des entiers.

Une fois un tel a trouvé, soit

$$r = a^{(p-1)/4}$$

On a alors

$$r^2 = a^{(p-1)/2} = -1$$

La complexité moyenne de cet algorithme est, en nombre d'opérations sur des entiers, $O(\log p)$. Histoire d'être un peu plus efficaces, on tire a au hasard, on calcule r, et si $r^2 = -1$ on renvoie r. Ceci évite d'avoir à calculer deux fois des puissances.

3.2 Puissances d'un nombre premier impair

Soit p un nombre premier congru à 1 modulo 4. Soit $n \geq 1$. Nous savons que $\mathcal{S}_{p^n}$ est de cardinal 2. Les deux éléments de cet ensemble étant opposés, il suffit d'en déterminer un.

Considérons la fonction $g : \mathbb{Z}_{p^n}^\times \longrightarrow \mathbb{Z}_p$ définie par

$$g(x) = \frac{x^2 - 1}{2x}$$

en convenant évidemment que si $u \in \mathbb{Z}_{p^n}$ et $v \in \mathbb{Z}_{p^n}^\times$, alors $u/v = uv^{-1}$.

Considérons la suite $(x_k)_{k \geq 1}$ d'éléments de $\mathbb{Z}_{p^n}$ définie comme suit. Tout d'abord, $x_1 = a + p^n\mathbb{Z}$ où $a \in \mathbb{Z}$ est tel que $a^2 + 1 \equiv 0 \bmod p$. Un tel a est déterminé par l'algorithme probabiliste du paragraphe précédent. Posons ensuite pour tout $k \geq 2$, $x_k = g(x_{k-1})$.

Proposition 16. *Pour tout $k \in [\![1, n]\!]$,*

- *x_k est bien défini.*
- *$x_k^2 + 1 \in p^k \mathbb{Z}_{p^n}$.*

Démonstration. Procédons par récurrence sur k. Pour $k = 1$, c'est par définition même de x_1. Soit $k \in [\![2, n]\!]$. Supposons que x_{k-1} est bien défini et $x_{k-1}^2 + 1 \in p^{k-1}\mathbb{Z}_{p^n}$. On a donc $x_{k-1} \notin p\mathbb{Z}_{p^n}$, donc $x_{k-1} \in \mathbb{Z}_{p^n}^\times$. De plus, comme p est impair, $2 \in \mathbb{Z}_{p^n}^\times$. On en déduit que $2x_{k-1} \in \mathbb{Z}_{p^n}^\times$, et donc que x_k est bien défini. Écrivons

$$2x_{k-1}x_k = x_{k-1}^2 - 1 = (x_{k-1}^2 + 1) - 2$$

Par l'hypothèse de récurrence,

$$x_{k-1}^2 + 1 = p^{k-1}u$$

où $u \in \mathbb{Z}_{p^n}$. On a donc

$$2x_{k-1}x_k = x_{k-1}^2 - 1 = p^{k-1}u - 2$$

En élevant au carré, il vient

$$\begin{aligned} 4x_{k-1}^2 x_k^2 &= p^{2k-2}u^2 - 4p^{k-1}u + 4 \\ &= p^{2k-2}u^2 - 4x_{k-1}^2 \end{aligned}$$

d'où

$$4x_{k-1}^2(x_k^2 + 1) = p^{2k-2}u^2$$

On a $4x_{k-1}^2 \mathbb{Z}_{p^n}^\times$, et donc

$$x_k^2 + 1 = p^{2k-2}v$$

où $v = u^2(4x_{k-1}^2)^{-1}$. Comme $k \geq 2$, on a $2k - 2 \geq k$, donc

$$x_k^2 + 1 \in p^k \mathbb{Z}_{p^n}$$

□

En prenant $k = n$ dans la proposition précédente, on obtient ainsi $x_n \in \mathbb{Z}_{p^n}$ tel que $x_n^2 + 1 \in p^n\mathbb{Z}_{p^n}$, c'est à dire tel que $x_n^2 + 1 = 0$. On obtient donc en $O(n)$ opérations sur des entiers un élément de S_{p^n}.

Remarque. Le calcul de x_k à partir de x_{k-1} peut être effectué modulo p^k. Ceci permet d'effectuer des opérations sur des entiers de taille moins importante.

Remarque. D'où vient la suite $(x_k)_{k\geq 1}$? Soit $P = X^2 + 1 \in \mathbb{Z}_{p^n}[X]$. On a pour tout $x \in \mathbb{Z}_{p^n}^\times$,

$$g(x) = x - \frac{P(x)}{P'(x)}$$

La définition de notre suite correspond donc à la méthode de Newton pour les racines d'une équation. La technique que nous avons utilisée fonctionne pour bien d'autres équations. La suite $(x_k)_{k\geq 1}$ est souvent appelée la *suite de Hensel* associée à x_1 et à P.

3.3 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 $\mathcal{S}_n$, il suffit de savoir faire la chose suivante : si $a, b \in \mathbb{N}^*$ sont premiers entre eux et que l'on connaît $\mathcal{S}_a$ et $\mathcal{S}_b$, déterminer S_{ab}.

Rappelons l'isomorphisme $\varphi : \mathbb{Z}_{ab} \longrightarrow \mathbb{Z}_a \times \mathbb{Z}_b$. On a

$$\mathcal{S}_{ab} = \varphi^{-1}(\mathcal{S}_a \times \mathcal{S}_b)$$

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 $y + a\mathbb{Z} \in \mathcal{S}_a$ et $z + b\mathbb{Z} \in \mathcal{S}_b$. 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,

$$\mathcal{S}_{ab} = \{uaz + vby + ab\mathbb{Z} : y + a\mathbb{Z} \in \mathcal{S}_a, z + b\mathbb{Z} \in \mathcal{S}_b\}$$

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 $\mathcal{S}_1 = \{0\}$, une simple boucle suffit pour calculer successivement les ensembles $\mathcal{S}_{p_1^{k_1} \dots p_j^{k_j}}$ pour $j \in [\![1, r]\!]$. On obtient ainsi $\mathcal{S}_n$ en r itérations.

3.4 Quelques exemples

Voici tout d'abord la liste des entiers $n \in [\![1, 100]\!]$ tels que $S_n \neq \emptyset$, ainsi que la liste correspondante des éléments de $\mathcal{S}_n$.

n	1	2	5	10	13	17	25	26	29	34	37	41	50
$\mathcal{S}_n$	0	1	2, 3	3, 7	5, 8	4, 13	7, 18	5, 21	12, 17	13, 21	6, 31	9, 32	7, 43

n	53	58	61	65	73	74	82	85	89	97
$\mathcal{S}_n$	23, 30	17, 41	11, 50	8, 18, 47, 57	27, 46	31, 43	9, 73	13, 38, 47, 72	34, 55	22, 75

Voici maintenant les éléments de $\mathcal{S}_n$ pour les puissances de 5.

n	5^n	S_{5^n}
1	5	$2, 3$
2	25	$7, 18$
3	125	$57, 68$
4	625	$182, 443$
5	3125	$1068, 2057$
6	15625	$1068, 14557$
7	78125	$32318, 45807$
8	390625	$110443, 280182$
9	1953125	$280182, 1672943$
10	9765625	$3626068, 6139557$

Prenons pour terminer un entier n qui a 4 diviseurs premiers, tous congrus à 1 modulo 4. Par exemple,

$$n = 5^2 \times 13^3 \times 17^2 \times 29^3 = 387134523425$$

L'ensemble $\mathcal{S}_n$ est de cardinal $2^4 = 16$:

$$\begin{aligned} \mathcal{S}_n \quad = \quad & \{21943183657, 68399326468, 74186250832, 117770446682, \\ & 120642393643, 164226589493, 170013513857, 170664866757, \\ & 216469656668, 217121009568, 222907933932, 266492129782, \\ & 269364076743, 312948272593, 318735196957, 365191339768 \end{aligned}$$

4 Le code Python

4.1 Racines carrées de -1 dans $\mathbb{Z}_p$

La fonction `racinem1` prend en paramètre un nombre premier p congru à 1 modulo 4. Elle renvoie une racine carrée de -1 modulo p. On utilise l'algorithme décrit dans la section 3.1. La fonction `racinem1` appelle une fonction `powermod` qui calcule des puissances modulo un entier.

```
def racinem1(p):
    while True:
        a = random.randint(1, p - 1)
        r = powermod(a, (p - 1) // 4, p)
        if (r ** 2 + 1) % p == 0:
            return r
```

4.2 Racines carrées de -1 dans $\mathbb{Z}_{p^n}$

La fonction `solve0` prend en paramètres un nombre premier p et un entier $n \geq 1$. Elle renvoie la liste des éléments de $\mathcal{S}_{p^n}$, en utilisant l'algorithme décrit dans la section 3.2. Elle appelle une fonction `invmod` qui calcule l'inverse d'un entier modulo un autre entier.

```
def solve0(p, n):
    if p == 2:
        if n == 1:
            return [1]
        else:
            return []
    elif p % 4 == 3:
        return []
    else:
        x = racinem1(p)
        for k in range(2, n + 1):
            y = invmod(2 * x, p ** k)
            x = ((x ** 2 - 1) * y) % (p ** k)
        return [x, p ** n - x]
```

4.3 Les solutions de (E_n)

Enfin, la fonction `solve` prend en paramètre un entier $n \geq 1$. Elle renvoie la liste des éléments de $\mathcal{S}_n$ triée dans l'ordre croissant. Elle utilise deux fonctions auxiliaires dont je ne donnerai pas le code ici :

- La fonction `facteurs` 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 relatifs 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 = []
        S2 = solve0(p, k)
        for y in S:
            for z in S2:
                x = (u * a * z + v * b * y) % (a * b)
                S1.append(x)
        a = a * b
        S = S1
    S.sort()
    return S
```