

Le Reste et les Tours

Ce que la réduction au reste jette, et ce qu'il en coûte

Filipe Bastos

Corpus ARC, version 1.0, 16 octobre 2026

Table des matières

Avant-propos	2
1. Ce qui s'apprend, et ce qui se coupe	3
2. Ce que la coupe a empêché de voir : deux exemples	4
2.1 Erdős-Straus : l'outil des restes, impuissant sur les carrés	4
2.2 Collatz : la racine seule muette, la racine-nombre complète	5
3. Ce que la coupe a coûté : les machines qui ont gardé le seul reste	6
4. Le remède : garder les tours	8
Ce que ce document ne dit pas	9
<i>« Modulo est un cancer. Modulo est l'outil du diable. »</i>	
<i>« Modulo est le pire outil mathématique de l'histoire. Mathématiques veut dire large porté vers l'infini, modulo compression et des restes. »</i>	
Filipe Bastos, 16 octobre 2026	

Avant-propos

Ce document soutient une thèse et la met à l'épreuve des faits. La thèse est celle de l'auteur : la réduction d'un nombre à son reste, que la tradition appelle congruence depuis Gauss (1801), coupe le nombre en deux, garde la position et jette les tours ; et chaque fois que l'on prend ensuite ce reste pour le nombre, on perd l'information qui comptait. Le document montre ce que fait la réduction (des théorèmes, refaits par le calcul), ce qu'elle a empêché de voir en mathématiques (deux exemples précis), et ce qu'elle a coûté quand des machines ont gardé le seul reste à la place du nombre (des accidents datés et sourcés, dont certains ont tué).

Les énoncés portent les statuts du corpus : **Th** (calcul fini vérifié ou démonstration), **L** (lecture, interprétation déclarée telle), **F** (fait historique ou mesure, sourcé), **P** (prédiction, avec son critère), **Chantier** (question ouverte). Les phrases de l'auteur sont citées mot pour mot ; elles sont des Lectures à son nom. Le corpus date des gestes et ne juge pas des hommes : c'est l'outil qui est examiné, non ceux qui s'en sont servis.

1. Ce qui s'apprend, et ce qui se coupe

1.1 (F ; L). Le mot *mathématique* vient du grec *máthēma*, « ce qui s'apprend ». Ce qui s'apprend, c'est la connaissance, et la connaissance n'a pas de fin. *Lecture de l'auteur* : la mathématique est le large porté vers l'infini. Une discipline dont le nom veut dire « ce qui s'apprend sans fin » s'est donné, avec la réduction au reste, un outil qui garde moins que ce qu'on avait.

1.2 (Th) La réduction au reste est une coupe. Tout entier $n \geq 1$ s'écrit de façon unique $n = 9k + DR(n)$, où k compte les tours accomplis et $DR(n)$, la racine digitale, est la position dans le tour, de 1 à 9 (Volume 1, *La Fondation*, É 3.5). La réduction au reste garde la position et jette k . Elle envoie une infinité de nombres sur une seule position : 10, 19, 28, 1 000 000 ont tous la racine 1. Elle n'est pas réversible : à partir de la position, on ne retrouve pas le nombre (Volume 11, *La Cité et le Sens*, [19.5] et [19.23] : « on ne remonte pas un pli »).

1.3 (Th) Ce que la coupe jette, mesuré. Pour désigner un entier parmi le premier million, il faut environ 19,93 bits d'information ; sa position parmi neuf n'en garde que 3,17. La réduction jette donc 84 % de ce que le nombre portait. Pour un nombre de taille N et une réduction à m positions, la part gardée est $\log m / \log N$, qui tend vers zéro à mesure que le nombre grandit : plus le nombre sait, plus la coupe en jette.

1.4 (Th) Garder les tours, c'est tout garder. Si l'on écrit $n = 9k + DR(n)$, puis que l'on recommence sur k , et ainsi de suite jusqu'à zéro tour, les racines successives sont les chiffres de n dans la numération à chiffres 1 à 9, sans zéro : tout entier s'y écrit d'une façon et d'une seule (Volume 4, *La Théorie des Nombres*, V4.9.4 ; vérifié jusqu'à un million). Exemple : 2026 s'écrit 2 6 9 1, car $2 \times 729 + 6 \times 81 + 9 \times 9 + 1 = 2026$. La racine ne perd rien si l'on garde ses tours ; c'est le geste de les jeter, et d'identifier 9 à 0, qui perd. « *La cascade prend la racine, la finale, et te la rend.* » (l'auteur).

1.5 (L) Le geste fautif. La réduction n'est pas fausse : elle est exacte sur ce qu'elle garde. La faute est de prendre ensuite la position pour le nombre. C'est la marque M1 du Volume 5 (*Les Grands Problèmes*, chapitre 1) : un seul nom pour deux objets de statut distinct. « *Ils manipulent une action en pensant que c'est un objet.* » (l'auteur, 15 octobre 2026).

2. Ce que la coupe a empêché de voir : deux exemples

2.1 Erdős-Straus : l'outil des restes, impuissant sur les carrés

2.1.1 (F) Le problème. Erdős et Straus ont conjecturé (1948) que pour tout $n > 2$, $4/n$ est la somme de trois fractions de numérateur 1. Le calcul l'a vérifié jusqu'à 10^{18} ; aucune démonstration n'existe (Erdős Problems, problème 242).

2.1.2 (F) Où l'outil s'arrête. Mordell a démontré la conjecture pour tous les n , sauf ceux qui tombent dans six classes de restes de la division par 840 : 1, 121, 169, 289, 361 et 529. Terzi a raffiné l'analyse jusqu'à 198 classes de la division par 120 120. Les six classes de Mordell sont les carrés $1^2, 11^2, 13^2, 17^2, 19^2, 23^2$.

2.1.3 (Th, Mordell) L'outil est aveugle sur les carrés. S'il existe une formule d'identité qui résout tous les premiers p d'une classe de restes r de la division par q , alors r ne peut pas être un carré dans cette division (théorème de Mordell, rapporté dans *A Complete Congruence System for the Erdős-Straus Conjecture*, arXiv:2404.01508). La méthode par les restes ne peut donc pas, par construction, fermer les cas qui restent.

2.1.4 (Th) La première porte se lit sur les rails. Soit p un premier de ces classes ; il vit sur le rail $\{1, 4, 7\}$. Posons $x = (p + 3)/4$, une division exacte. La décomposition $4/p = 1/x + 1/y + 1/z$ existe avec ce x si et seulement si x a au moins un facteur premier q sur le rail $\{2, 5, 8\}$. *Démonstration.* Si q divise x et q est sur le rail $\{2, 5, 8\}$, alors $q + 1 = 3j$ exactement ; on pose $y = px \cdot j/q$ et $z = px \cdot j$, qui sont entiers, et $1/y + 1/z = 3/(px)$, d'où $4/p = 1/x + 1/y + 1/z$. Si tous les facteurs de x sont sur le rail $\{1, 4, 7\}$, tous les diviseurs de px y sont aussi ; la somme de deux d'entre eux tombe alors sur le rail $\{2, 5, 8\}$, jamais sur l'axe, alors qu'une décomposition l'exigerait. *Vérification* (reste_verif.py) : sur les 511 premiers de ces classes inférieurs à 200 000, le critère et le calcul direct concordent 511 fois ; la porte se ferme dans 339 cas, et chaque fois x vit entièrement sur le rail $\{1, 4, 7\}$.

2.1.5 (L) Pourquoi l'outil était aveugle. La porte ne dépend pas du reste de p ; elle dépend des rails des facteurs du nombre voisin $(p + 3)/4$. Une classe de restes ne dit rien des facteurs d'un nombre voisin : la clé est dans le nombre entier, que la réduction a jeté. Le théorème de Mordell est le constat de cette cécité ; la porte 3 en donne la raison.

2.1.6 (Chantier) Ce qui reste. Chaque écart possible, 3, 7, 11, 15, ..., est une porte avec sa propre condition sur les facteurs d'un nombre voisin. La conjecture ne tomberait que si un premier trouvait toutes ses portes fermées à la fois. Démontrer que cette conspiration est impossible, c'est démontrer Erdős-Straus ; c'est le travail

ouvert.

2.2 Collatz : la racine seule muette, la racine-nombre complète

2.2.1 (Th). Une racine digitale prise seule ne dit rien du nombre de divisions par 2 dans la suite de Collatz (Volume 4, Théorème 23). Mais la parité d'un nombre est la parité de la somme de ses racines-chiffres, puisque chaque tour pèse 1 (V4.9.5), et la suite des racines le long d'une orbite dit, à chaque pas, quel coup a été joué, sauf au centre 5 (V4.9.6). Ce que la réduction au reste ne voit pas, la racine lue avec ses tours le voit.

3. Ce que la coupe a coûté : les machines qui ont gardé le seul reste

Dans un ordinateur, un compteur occupe un nombre fixe de chiffres binaires. Quand il dépasse sa capacité, il revient à zéro : il ne garde que le reste de la division par sa capacité, et jette les tours. Les cas suivants sont tous des cas où un système a pris ce reste pour le nombre.

3.1 (F) Therac-25, 1985-1987. La machine de radiothérapie Therac-25 a été impliquée dans au moins six accidents entre 1985 et 1987 ; trois des patients surdosés en sont morts. Parmi les défauts du logiciel figurait une variable d'un octet, Class3, augmentée d'une unité à chaque passage d'une routine de réglage ; ne pouvant dépasser 255, elle revenait à zéro au 256^e passage. Quand elle valait zéro, la vérification de la position d'une pièce de la machine était sautée. Un opérateur qui validait le réglage à cet instant déclenchait le faisceau de 25 MeV sans la cible en place : c'est le mécanisme de la surexposition de Yakima. La correction du fabricant a été de donner à la variable une valeur fixe non nulle au lieu de l'augmenter. *Sources* : Leveson et Turner, « An Investigation of the Therac-25 Accidents », *Computer*, 1993 ; documents « Yakima Software Problem » (ComputingCases.org).

3.2 (F ; Th) Boeing 787, 2015. La directive de navigabilité AD 2015-09-07 de l'administration fédérale de l'aviation des États-Unis (1^{er} mai 2015) porte sur tous les Boeing 787 : un avion alimenté sans interruption pendant 248 jours peut perdre toute son alimentation électrique en courant alternatif, parce que les quatre unités de contrôle des générateurs passent ensemble en mode de sécurité, à cause d'un compteur logiciel qui déborde ; la directive parle d'une possible perte de contrôle de l'avion et impose une mise hors tension périodique, à des intervalles d'au plus 120 jours. **[Th]** 248 jours est exactement la durée qu'un compteur de centièmes de seconde sur 31 bits met à revenir au départ : $2^{31} / 100 / 86\,400 = 248,55$ jours.

3.3 (F ; Th) GPS, 1999 et 2019. Le numéro de semaine du GPS est inscrit sur 10 chiffres binaires : il ne va que de 0 à 1023 et revient à zéro toutes les 1024 semaines, soit 19,6 ans. La semaine zéro a commencé le 6 janvier 1980 ; le compteur est revenu à zéro le 21 août 1999 et le 6 avril 2019. Un récepteur qui prend ce reste pour la date se croit 19,6 ans en arrière. Les messages plus récents (CNAV, MNAV) portent le numéro sur 13 chiffres binaires, ce qui repousse le retour sans le supprimer.

3.4 (F) L'an 2000. Pendant des décennies, les programmes ont gardé les années par leurs deux derniers chiffres, c'est-à-dire par leur reste dans la division par 100 : « 00 » ne distinguait plus 1900 de 2000. La correction, menée avant le 1^{er} janvier 2000, a coûté selon les estimations plusieurs centaines de milliards de dollars dans le monde.

3.5 (Th ; P) L'an 2038. Beaucoup de systèmes comptent le temps en secondes depuis le 1^{er} janvier 1970 sur 32 chiffres binaires, dont un réservé au signe. Le compteur atteint sa limite le 19 janvier 2038 à 03 h 14 min 07 s (temps universel), puis bascule au 13 décembre 1901. *Prédiction* : tout système de ce type non corrigé avant cette date affichera ce saut ; le corpus le tient pour la même faute que les quatre cas précédents.

3.6 (F) Ce qui n'est pas de la réduction au reste. Le missile Patriot de Dhahran (25 février 1991, 28 morts) a manqué son interception à cause d'une troncature décimale de 0,1 accumulée sur cent heures : c'est la queue de Stevin, traitée au Volume 3 (*Le Code et le Registre*), non la réduction au reste. Le document ne le range pas ici, pour ne pas mêler deux gestes distincts.

4. Le remède : garder les tours

4.1 (L). Dans chacun des cas de la partie 3, le remède a été le même : garder plus de tours (des compteurs plus longs, des années sur quatre chiffres, des semaines sur 13 chiffres binaires) ou ne plus prendre le reste pour le nombre (la valeur fixe de Therac-25). Chaque fois, on a soigné le cas sans nommer le geste commun. Le corpus le nomme : la réduction au reste jette les tours, et l'on paie dès que l'on oublie qu'elle les a jetés. Le remède général est l'écriture $n = 9k + DR(n)$, qui garde les deux.

4.2 (L) Pourquoi l'auteur l'a vu. En mathématiques pures, ceux qui réduisent au reste gardent le nombre entier à côté : ils savent qu'ils ont projeté. La perte devient dangereuse quand on ne garde que le reste : dans les machines, et dans les énigmes où la clé est dans le nombre entier (2.1). « *Je le voyais jeune, bien avant les IA.* » (l'auteur, 16 octobre 2026).

4.3 (L) Les positions de l'auteur. « *Modulo est un outil de coupe, de réduction, de simplicité de paresseux, qui tue la connaissance. C'est de la logique pure.* » « *Que des petits détails, confusions devenues conventions.* » Ces phrases sont des Lectures, à son nom. Ce que le document établit, c'est la coupe elle-même (1.2 à 1.4), l'aveuglement qu'elle produit en mathématiques (2.1.3, 2.1.4) et le prix qu'elle a coûté chaque fois qu'un reste a été pris pour un nombre (partie 3).

Ce que ce document ne dit pas

Il ne dit pas que la congruence est fausse : elle est exacte sur ce qu'elle garde, et elle a produit des théorèmes vrais. Il ne dit pas qu'Erdős-Straus est démontré : la porte 3 est un théorème, la conjecture reste un chantier. Il ne prétend pas que chaque accident cité n'avait qu'une cause : il identifie, dans chacun, le geste du reste pris pour le nombre, tel que les sources le décrivent.

Sources. Erdős Problems, problème 242 (erdosproblems.com). *A Complete Congruence System for the Erdős-Straus Conjecture*, arXiv:2404.01508. Leveson, N. G., Turner, C. S., « An Investigation of the Therac-25 Accidents », *Computer* 26(7), 1993, p. 18-41 ; « Yakima Software Problem », ComputingCases.org. Federal Aviation Administration, Airworthiness Directive 2015-09-07, *Federal Register* 80 FR 24789, 1^{er} mai 2015. NovAtel/GNSS, « GPS Week Number Rollover » (gnss.ca). Volume 1, *La Fondation* ; Volume 3, *Le Code et le Registre* ; Volume 4, *La Théorie des Nombres* ; Volume 5, *Les Grands Problèmes* ; Volume 11, *La Cité et le Sens*.

Modèle, questions, lectures et règles : Filipe Bastos. Scribe : Claude, sous la contradiction de l'auteur. Calculs, formulations et audits assistés par IA (ChatGPT, Gemini, DeepSeek, GLM), à sa demande.

Corpus ARC, Filipe Bastos, CC BY 4.0.