

## “ Sur les développements décimaux illimités de rationnels ”

Eliane COUSQUER (USTL)

*Avoir soi-même éprouvé l'intérêt et la motivation que suscite un problème ouvert dont on n'a ni la réponse ni de piste de résolution, avoir à élaborer sa propre stratégie, est un très bon outil de formation initiale et continue des enseignants, pour les inciter à mettre les élèves ou étudiants en situation de recherche.*

### Notre pratique à l'IREM et à l'IUFM de Lille

Lors de l'année 1995-1996, nous avons développé à l'occasion d'un stage Irem de formation continue à Lille sur le thème des nombres des «activités de découverte». Il s'agit de séances relativement longues (environ trois heures) où les enseignants se trouvent confrontés à un problème ouvert pour eux, inspiré le plus souvent par un problème historique. Les enseignants se sont engagés avec enthousiasme dans cette activité d'expérimentation, de formulation de conjectures puis de démonstration lorsque les conjectures émises résistaient au débat. Ces mêmes activités ont été expérimentées également en formation initiale des maîtres comme thème de mémoires, et en formation initiale à différents niveaux (collège, lycée, Deug) et présentées dans différents colloques (Rouen, Nantes).

### Activités de découverte sur les nombres

Alors que l'arithmétique va être introduite dans les programmes de lycée<sup>1</sup>, il est important de se rendre compte que c'est un domaine où il est possible de développer un caractère expérimental dans l'enseignement des mathématiques. Le thème des nombres permet de poser des problèmes d'apparence simple et l'existence des moyens de calcul actuel, en particulier les calculatrices, permet d'obtenir rapidement des résultats expérimentaux qui aident à cerner le problème et à formuler des conjectures, à les tester car la plupart d'entre elles ne résistent pas à l'épreuve des faits.

<sup>1</sup>nous recommandons à tous les enseignants et aux étudiants l'excellent livre *Introduction à la théorie des nombres* par Jean Marie De Koninck et Armel Mercier.

## Présentation de l'activité choisie dans cet atelier

Il s'agit de trouver des lois concernant le nombre de chiffres de la période et le nombre de chiffres qui précèdent la période dans les parties décimales des développements décimaux illimités des rationnels. Comme vous le constaterez vous-mêmes sur l'activité présentée ici, le réinvestissement est possible à tous les niveaux d'enseignement pour des activités destinées aux élèves ou aux étudiants.

## Origine historique de cette activité

L'idée de départ peut être trouvée dans le livre *Disquisitiones arithmeticae* (1801) de Gauss (1777-1855) qui y a exposé la théorie des congruences, dans la troisième section et développé dans la sixième différentes applications dont la théorie des développements décimaux illimités<sup>2</sup>. Je pense avec l'activité présentée ici être fidèle à un aspect des recherches de Gauss qui a beaucoup expérimenté sur des valeurs particulières, par exemple en confectionnant des tables de valeurs, que nous analyserons, avant d'induire des résultats qu'il démontrait ensuite ou pour lesquels il indiquait ne pas avoir encore une démonstration générale. La méthode ici utilisée présente donc aussi un intérêt historique.

Il n'est pas question ici de faire un exposé d'histoire de l'arithmétique<sup>3</sup>, mais d'illustrer dans ce chapitre une propriété très particulière de l'arithmétique : c'est un domaine où les énoncés paraissent simples, ce qui ne veut pas dire que leur solution le soit, et il y a, surtout avec les moyens de calculs actuels, même de simples calculettes, des possibilités d'expérimentation pour émettre des conjectures. Cette science est très vivante à l'heure actuelle où les problèmes de codage et de cryptographie mêlent étroitement informatique, algèbre et arithmétique<sup>4</sup>.

## Déroulement de l'atelier à Nantes

Alors que l'atelier à Lille se déroulait sur trois heures pour la seule activité de découverte, j'ai voulu développer la partie historique et donc partagé l'atelier à Nantes en deux périodes de une heure trente : une pour l'aspect

<sup>2</sup>qui figure pages 388 à 398 de la traduction du livre de Gauss paru aux éditions Blanchard sous le titre «*Recherches Arithmétiques*».

<sup>3</sup>Il en existe une très bonne en anglais : *Number theory and its history*, par Oystein Ore.

<sup>4</sup>cf *Cours d'algèbre, primalité, divisibilité, codes* de Michel Demazure.

découverte, une sur le texte de Gauss lui-même qui a marqué un tournant dans l'histoire de l'arithmétique.

À chaque étape, je demande une lecture active. Une fois le problème en tête, fermez ce livre et essayez, en faisant les calculs que je vous propose, de découvrir vous-même les propriétés : les mathématiciens appellent cela émettre des conjectures. Ensuite, vous confronterez ce que vous avez trouvé à la synthèse qui suit. Et nous recommencerons notre cheminement ensemble jusqu'à la prochaine expérimentation. Pour faire ce travail, une calculette avec les quatre opérations suffit. Notez au fur et à mesure vos résultats.

## Les nombres premiers

Un entier  $a$  divise un autre entier  $b$  si on peut trouver un entier  $c$  tel que  $b = ac$ ; on note  $a|b$ ; 1 divise n'importe quel entier, et tout entier se divise lui-même : si  $a = b$ , on prend  $c = 1$ . Par exemple 5 divise 15 puisque  $15 = 3 \times 5$ , par contre 7 ne divise pas 15. Parmi les entiers, on distingue les nombres premiers dont les seuls diviseurs sont 1 et lui-même. 1 n'est pas compté dans les nombres premiers. Nous allons chercher tous les nombres premiers par exemple de 1 à 100 à l'aide d'une méthode connue depuis l'antiquité sous le nom de *crible d'Ératosthène*. Tous les entiers de 2 à 100 sont écrits dans le tableau suivant.

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Vous barrez tous les multiples de 2 (sauf 2) : ils ne sont pas des nombres premiers. Le premier nombre suivant 2 non barré est 3, c'est un nombre premier. Barrez tous ses multiples. Le premier nombre suivant non barré est 5. C'est un nombre premier, barrez ses multiples etc... Les nombres restant sont des nombres premiers. Il reste les nombres premiers :

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53  
59 61 67 71 73 79 83 89 97

On sait beaucoup de choses sur les nombres premiers, mais on se pose encore beaucoup de questions. On sait calculer de très grands nombres premiers avec les ordinateurs, mais on ne sait pas, pour des nombres immenses, les décomposer en facteurs. Les algorithmes de cryptage reposent là-dessus.

Tous les nombres se décomposent de façon unique en un produit de facteurs premiers, ordonnés du plus petit au plus grand. Par exemple

$$8820 = 2^2 \times 3^2 \times 5 \times 7^2$$

Quelque soit la façon dont on procède, on obtiendra toujours cette décomposition. Nous allons nous intéresser aux nombres rationnels que nous écrirons toujours sous forme de fractions irréductibles. Par exemple, nous simplifions la fraction  $\frac{24}{60}$  en la fraction  $\frac{2}{5}$ . L'usage de la décomposition en facteurs premiers permet de simplifier la fraction par les facteurs communs au numérateur et au dénominateur. Les caleuses de collège actuelles disposent aussi d'une fonction de simplification des fractions.

## Développement décimal des nombres rationnels

Un premier problème est de prendre conscience de la différence entre nombre décimal et développement décimal illimité. Les nombres décimaux sont des nombres qui peuvent s'écrire sous forme d'une fraction dont le dénominateur se présente sous la forme  $2^\alpha \times 5^\beta$ , (avec seulement 2 et (ou) 5 dans sa décomposition en facteurs premiers). Les nombres décimaux possèdent deux développements décimaux illimités, l'un fini, (avec des 0 indéfiniment), l'autre avec des 9 indéfiniment<sup>5</sup>. Nous laisserons les décimaux de côté dans cette activité.

Les nombres rationnels non décimaux possèdent un unique développement décimal illimité périodique : si on pose la division du numérateur par le dénominateur, le nombre des restes possibles est inférieur au dénominateur, au bout d'un moment la division boucle. Le développement décimal d'un rationnel comporte une partie entière suivie d'une partie fractionnaire. On s'intéressera à la seule partie fractionnaire, ce qui revient à s'intéresser aux fractions irréductibles, entre 0 et 1, c'est-à-dire aux fractions dont le numérateur est inférieur au dénominateur. La partie fractionnaire comporte une partie périodique de  $i$  chiffres, précédée d'un certain nombre  $n$  de chiffres.

<sup>5</sup>Par exemple

$$\frac{17}{50} = \frac{34}{100} = 0,34 = 0,34000\dots = 0,33999\dots$$

## Activité proposée

L'activité se propose de chercher si l'on peut trouver des lois générales sur le nombre  $i$  de chiffres de la période, et sur le nombre  $n$  de chiffres précédant la partie périodique du développement, en fonction des entiers  $p$  et  $q$ .

Nous vous proposons de chercher le développement périodique illimité des fractions  $\frac{p}{q}$  irréductibles, ( $p < q$ ), pour  $q$  variant par exemple de 3 à 17. Nous nous intéressons aux fractions irréductibles inférieures à 1 de dénominateurs 3, 6, 7, 9, 11, 12, 13, 14, 15, 17, pour avoir des fractions non décimales.

Déterminez les nombres  $n$  et  $i$  correspondant à chacune des fractions et essayez d'émettre des conjectures, sur les nombres  $n$  et  $i$ .

Trouvez-vous mêmes un critère pour grouper les développements des fractions de dénominateur  $q$  en familles. Combien trouvez-vous de familles ? Là-aussi, on peut émettre des conjectures et essayer de les démontrer.

Testez vos conjectures et ce que vous avez compris sur les fractions de dénominateurs compris entre 19 et 29.

Toute cette pratique de calcul nous sera utile pour comprendre le texte de GAUSS.

## Résultats expérimentaux et conjectures

Pour chaque valeur du dénominateur  $q$ , nous allons lister ces fractions et donner leurs développements. Nous mettrons en évidence le couple  $(n, i)$  et les familles apparues dans le calcul. On surlignera la période pour indiquer que celle-ci est répétée indéfiniment.

**Fractions de dénominateur 3 :** Deux développements purement périodiques (sans chiffres avant la période) et comportant une période d'un seul chiffre.

$$\frac{1}{3} = 0,33333\dots = 0,\overline{3} \quad (0, 1) \quad ; \quad \frac{2}{3} = 0,66666\dots = 0,\overline{6} \quad (0, 1)$$

**Fractions de dénominateur 6 :** Deux développements comportant un chiffre avant la période et une période d'un seul chiffre.

$$\frac{1}{6} = 0,16666\dots = 0,1\overline{6} \quad (1, 1) \quad ; \quad \frac{5}{6} = 0,83333\dots = 0,8\overline{3} \quad (1, 1)$$

On retrouve les parties périodiques apparues pour le dénominateur 3.

**Fractions de dénominateur 7 :** Lorsqu'on calcule les six développements, on constate qu'aucun n'a de chiffres avant la période, que tous ont une période de 6 chiffres. Par contre la disposition suivante montre que les développements ont des périodes qui se déduisent les unes des autres par

permutation circulaire. Nous dirons que nous avons une seule famille de développements.

$$\frac{1}{7} = 0,142857142857\dots = 0,\overline{142857} \quad (0,6)$$

$$\frac{3}{7} = 0,428571428571\dots = 0,\overline{428571} \quad (0,6)$$

$$\frac{2}{7} = 0,285714285714\dots = 0,\overline{285714} \quad (0,6)$$

$$\frac{6}{7} = 0,857142857142\dots = 0,\overline{857142} \quad (0,6)$$

$$\frac{4}{7} = 0,571428571428\dots = 0,\overline{571428} \quad (0,6)$$

$$\frac{5}{7} = 0,714285714285\dots = 0,\overline{714285} \quad (0,6)$$

**Fractions de dénominateur 9 :** Lorsqu'on calcule les six développements, on constate qu'aucun n'a de chiffres avant la période, que tous ont une période d'un seul chiffre.

$$\frac{1}{9} = 0,\overline{1}; \quad \frac{2}{9} = 0,\overline{2}; \quad \frac{4}{9} = 0,\overline{4}; \quad \frac{5}{9} = 0,\overline{5}; \quad \frac{7}{9} = 0,\overline{7}; \quad \frac{8}{9} = 0,\overline{8}; \quad (0,1)$$

**Fractions de dénominateur 11 :** Lorsqu'on calcule les dix développements, on constate qu'aucun n'a de chiffres avant la période, que tous ont une période de deux chiffres. On trouve six familles de deux développements chacune.

$$\frac{1}{11} = 0,090909\dots = 0,\overline{09} \quad ; \quad \frac{10}{11} = 0,909090\dots = 0,\overline{90} \quad (0,2)$$

$$\frac{2}{11} = 0,181818\dots = 0,\overline{18} \quad ; \quad \frac{9}{11} = 0,818181\dots = 0,\overline{81} \quad (0,2)$$

$$\frac{3}{11} = 0,272727\dots = 0,\overline{27} \quad ; \quad \frac{8}{11} = 0,727272\dots = 0,\overline{72} \quad (0,2)$$

$$\frac{4}{11} = 0,363636\dots = 0,\overline{36} \quad ; \quad \frac{7}{11} = 0,636363\dots = 0,\overline{63} \quad (0,2)$$

$$\frac{5}{11} = 0,454545\dots = 0,\overline{45} \quad ; \quad \frac{6}{11} = 0,545454\dots = 0,\overline{54} \quad (0,2)$$

**Fractions de dénominateur 12 :** Quatre développements où l'on constate que tous ont une période de un chiffre, précédée par deux chiffres. On retrouve la partie périodique des fractions de dénominateurs 3.

$$\frac{1}{12} = 0,08\overline{3}; \quad \frac{5}{12} = 0,41\overline{6}; \quad \frac{7}{12} = 0,58\overline{3}; \quad \frac{11}{12} = 0,91\overline{6} \quad (2,1)$$

**Fractions de dénominateur 13 :** Douze développements; on constate qu'aucun n'a de chiffres avant la période, que tous ont une période de six chiffres. Il y a deux familles de six fractions chacune.

$$\frac{1}{13} = 0,076923 \quad (0,6) \quad \frac{2}{13} = 0,153846 \quad (0,6)$$

$$\frac{10}{13} = 0,769230 \quad (0,6) \quad \frac{7}{13} = 0,538461 \quad (0,6)$$

$$\frac{9}{13} = 0,692307 \quad (0,6) \quad \frac{5}{13} = 0,384615 \quad (0,6)$$

$$\frac{12}{13} = 0,923076 \quad (0,6) \quad \frac{11}{13} = 0,846153 \quad (0,6)$$

$$\frac{3}{13} = 0,230769 \quad (0,6) \quad \frac{6}{13} = 0,461538 \quad (0,6)$$

$$\frac{4}{13} = 0,307692 \quad (0,6) \quad \frac{8}{13} = 0,615384 \quad (0,6)$$

**Fractions de dénominateur 14 :** Six développements qui ont un chiffre avant la période, une période de six chiffres et forment une seule famille. On remarque qu'on obtient les mêmes périodes que pour les fractions de dénominateur 7.

$$\frac{1}{14} = 0,071428\overline{5}; \quad \frac{3}{14} = 0,214285\overline{7}; \quad \frac{9}{14} = 0,642857\overline{1} \quad (1,6)$$

$$\frac{13}{14} = 0,928571\overline{4}; \quad \frac{11}{14} = 0,785714\overline{2}; \quad \frac{5}{14} = 0,357142\overline{8} \quad (1,6)$$

**Fractions de dénominateur 15 :** Huit développements qui ont un chiffre avant la période et une période de un chiffre, on retrouve les périodes des fractions de dénominateurs 3.

$$\frac{2}{15} = 0,1\overline{3} \quad \frac{8}{15} = 0,5\overline{3} \quad \frac{11}{15} = 0,7\overline{3} \quad \frac{14}{15} = 0,9\overline{3} \quad (1,1)$$

$$\frac{1}{15} = 0,0\overline{6} \quad \frac{4}{15} = 0,2\overline{6} \quad \frac{7}{15} = 0,4\overline{6} \quad \frac{13}{15} = 0,8\overline{6} \quad (1,1)$$

**Fractions  $p/17$  :** On fait le calcul de  $1/17$  qui dépasse les capacités de toutes les calculettes ce qui amène à se poser la question soit de poser la division, soit de travailler par étapes. On divise  $10^7$  par 17 en prenant soin d'écrire le reste.

$$\begin{aligned} 10^7 &= 17 \times 588235 + 5 & ; & \quad \frac{1}{17} = \frac{1}{10^7} (588235 + \frac{5}{17}) \\ 5 \times 10^7 &= 17 \times 2941176 + 8 & ; & \quad \frac{5 \times 10^7}{17 \times 10^{14}} = \frac{1}{10^{14}} (2941176 + \frac{8}{17}) \\ 8 \times 10^2 &= 17 \times 47 + 1 & ; & \quad \frac{8 \times 10^2}{17 \times 10^{16}} = \frac{1}{10^{16}} (47 + \frac{1}{17}) \end{aligned}$$

On est sûr que l'opération boucle à ce niveau, puisqu'on a obtenu le reste 1. On a une seule famille :  $\frac{1}{17} = 0,058\,823\,529\,411\,764\,7$

On peut remarquer que la méthode précédente est aussi une méthode qui permet de justifier qu'on a obtenu la période. On sait que le nombre de chiffres de la période est inférieur ou égal au dénominateur. Sauf cas très particuliers pour de petites valeurs de  $q$ , on ne peut se contenter de lire la période sur la calculette.

### Conjecture 1

Les nombres  $n$  et  $i$  dépendent du seul dénominateur et non du numérateur.

### Conjecture 2

Le nombre de chiffres avant la période dépend de la divisibilité du dénominateur par 2 ou 5. Seules les fractions de dénominateurs 6, 12, 14, 15 ont des chiffres avant la période. On peut émettre la conjecture que  $n$  est non nul pour les dénominateurs divisibles par 2 ou par 5, ce qui est cohérent avec le rôle joué par ces deux nombres pour les nombres décimaux. Si on décompose  $q$  en produit  $q = 2^a 5^b q'$  avec  $q'$  premier avec 2 et 5, on peut conjecturer que la partie périodique ne dépend que de  $q'$  et que le nombre  $n$  est lié aux exposants  $a$  et  $b$  de 2 et 5; avant de faire la démonstration générale montrons ce qui se passe sur les exemples précédents.

$$\begin{aligned} 6 &= 2 \times 3 \quad (n = 1) & ; & \quad 12 = 4 \times 3 \quad (n = 2) \\ 14 &= 2 \times 7 \quad (n = 1) & ; & \quad 15 = 5 \times 3 \quad (n = 1) \end{aligned}$$

### Fractions de dénominateur 6 :

$$\frac{1}{6} = 0,16666\dots = \frac{5}{10 \times 3} = \frac{1}{10} (1 + \frac{2}{3}) \quad ; \quad \frac{5}{6} = 0,83333\dots = \frac{25}{10 \times 3} = \frac{1}{10} (8 + \frac{1}{3})$$

### Fractions de dénominateur 12 :

$$\begin{aligned} \frac{1}{12} &= 0,08\bar{3} = \frac{25}{100 \times 3} = \frac{1}{100} (8 + \frac{1}{3}) & ; & \quad \frac{5}{12} = 0,41\bar{6} = \frac{125}{100 \times 3} = \frac{1}{100} (41 + \frac{2}{3}) \\ \frac{7}{12} &= 0,58\bar{3} = \frac{175}{100 \times 3} = \frac{1}{100} (58 + \frac{1}{3}) & ; & \quad \frac{11}{12} = 0,91\bar{6} = \frac{275}{100 \times 3} = \frac{1}{100} (91 + \frac{2}{3}) \end{aligned}$$

### Fractions de dénominateur 14 :

$$\begin{aligned} \frac{1}{14} &= 0,071428\bar{5} = \frac{5}{10 \times 7} = \frac{1}{10} (0 + \frac{5}{7}) & ; & \quad \frac{3}{14} = 0,214285\bar{7} = \frac{15}{10 \times 7} = \frac{1}{10} (2 + \frac{1}{7}) \\ \frac{5}{14} &= 0,357142\bar{8} = \frac{25}{10 \times 7} = \frac{1}{10} (3 + \frac{4}{7}) & ; & \quad \frac{9}{14} = 0,642857\bar{1} = \frac{45}{10 \times 7} = \frac{1}{10} (6 + \frac{3}{7}) \\ \frac{11}{14} &= 0,785714\bar{2} = \frac{55}{10 \times 7} = \frac{1}{10} (7 + \frac{6}{7}) & ; & \quad \frac{13}{14} = 0,928571\bar{4} = \frac{65}{10 \times 7} = \frac{1}{10} (9 + \frac{2}{7}) \end{aligned}$$

### Fractions de dénominateur 15 :

$$\begin{aligned} \frac{1}{15} &= 0,0\bar{6} = \frac{2}{10 \times 3} = \frac{1}{10} (0 + \frac{2}{3}) & ; & \quad \frac{2}{15} = 0,1\bar{3} = \frac{4}{10 \times 3} = \frac{1}{10} (1 + \frac{1}{3}) \\ \frac{4}{15} &= 0,2\bar{6} = \frac{8}{10 \times 3} = \frac{1}{10} (2 + \frac{2}{3}) & ; & \quad \frac{7}{15} = 0,4\bar{6} = \frac{14}{10 \times 3} = \frac{1}{10} (4 + \frac{2}{3}) \\ \frac{8}{15} &= 0,5\bar{3} = \frac{16}{10 \times 3} = \frac{1}{10} (5 + \frac{1}{3}) & ; & \quad \frac{11}{15} = 0,7\bar{3} = \frac{22}{10 \times 3} = \frac{1}{10} (7 + \frac{1}{3}) \\ \frac{13}{15} &= 0,8\bar{6} = \frac{26}{10 \times 3} = \frac{1}{10} (8 + \frac{2}{3}) & ; & \quad \frac{14}{15} = 0,9\bar{3} = \frac{28}{10 \times 3} = \frac{1}{10} (9 + \frac{1}{3}) \end{aligned}$$

**Démonstration générale :** On décompose  $q$  en un produit  $2^a 5^b q'$  avec  $q'$  premier avec 10 :

$$\begin{aligned} a = b & \quad \frac{p}{q} = \frac{1}{10^a} \times \frac{p}{q'} & \quad p = mq' + r & \quad \text{et} & \quad \frac{p}{q} = \frac{1}{10^a} \times (m + \frac{r}{q'}) \\ a < b & \quad \frac{p}{q} = \frac{1}{10^b} \times \frac{p \times 2^{b-a}}{q} & \quad p \times 2^{b-a} = mq' + r & \quad \text{et} & \quad \frac{p}{q} = \frac{1}{10^b} \times (m + \frac{r}{q'}) \\ a > b & \quad \frac{p}{q} = \frac{1}{10^a} \times \frac{p \times 5^{a-b}}{q} & \quad p \times 5^{a-b} = mq' + r & \quad \text{et} & \quad \frac{p}{q} = \frac{1}{10^a} \times (m + \frac{r}{q'}) \end{aligned}$$

L'entier  $m$  est inférieur à  $10^a$  dans le premier cas, à  $10^b$  dans le deuxième et à  $10^a$  dans le troisième car la fraction  $\frac{p}{q}$  est inférieure à 1. Nous allons justifier que  $\frac{r}{q'}$  admet un développement purement périodique, ce qui fait l'objet de la conjecture suivante. Admettons le momentanément. Alors, on voit que le nombre de chiffres avant la période est donné par  $n = \sup(a, b)$  et que le décimal avant la période est  $\frac{m}{10^n}$ .

### Conjecture 3

Le développement d'une fraction  $\frac{p}{q}$  irréductible inférieure à 1 où  $q$  est premier avec 10 est purement périodique (pas de chiffres avant la période), et le nombre de chiffres de la période ne dépend que de  $q$ . C'est ce qu'on a vu sur les fractions de dénominateur 3, 7, 9, 11, 13, 17.

**Fractions de dénominateur 7 :** Pour mieux comprendre ce qui se passe, nous allons poser la division de  $\frac{1}{7}$ .

$$\begin{array}{r}
 10 \\
 30 \\
 20 \\
 60 \\
 40 \\
 50 \\
 1
 \end{array}
 \begin{array}{r}
 7 \\
 \hline
 0,142857
 \end{array}$$

Observons la suite des restes partiels. Les développements des différentes fractions  $\frac{p}{7}$  s'obtiennent pour  $\frac{3}{7}$  en supprimant le premier chiffre du quotient après la virgule, pour  $\frac{2}{7}$ , en en supprimant deux, etc ce qui produit une permutation circulaire à partir de la période de  $\frac{1}{7}$ , et explique l'ordre dans lequel nous avons écrit ces développements. Comme les restes partiels comportent tous les entiers entre 1 et 6, on a une seule famille, et une seule division suffit à connaître tous les développements  $\frac{p}{7}$ . On remarque que l'opération boucle quand on obtient le reste 1.

Dorénavant nous écrirons «en ligne» cette division en faisant apparaître les chiffres successifs du quotient et du reste.

**Fractions de dénominateur 7 :**

quotient	0, 1 4 2 8 5 7
reste	1 3 2 6 4 5 1

**Fractions de dénominateur 17 :** On fait le calcul de  $1/17$

quotient	0, 0 5 8 8 2 3 5 2 9 4 1 1 7 6 4 7
restes	1 10 15 14 4 6 9 5 16 7 2 3 13 11 8 12 1

L'ordre des restes permettra de retrouver le développement de toutes les fractions  $p/17$ , sans refaire de calcul. Par exemple pour obtenir le développement de  $6/17$  on supprime dans le développement de  $1/17$  les 5 premiers chiffres après la virgule, (ne pas oublier que le développement est infini).

**Fractions de dénominateur 13 :** Faisons d'abord la division  $\frac{1}{13}$ , en faisant apparaître les restes successifs.

quotient	0, 0 7 6 9 2 3
reste	1 10 9 12 3 4 1

On retrouve la famille :  $1/13, 10/13, 9/13, 12/13, 3/13, 4/13$ . La fraction  $\frac{2}{13}$  ne figure pas dans cette liste. Cherchons son développement en effectuant la division de 2 par 13

quotient	0, 1 5 3 8 4 6
reste	2 7 5 11 6 8 2

On trouve la deuxième famille :  $2/13, 7/13, 5/13, 11/13, 6/13, 8/13$ . Les restes s'obtiennent en multipliant par 2 les restes de la première famille et en réduisant modulo 13<sup>6</sup>.

**Démonstration générale :** Si nous cherchons à quel moment une division telle que  $1 : q$  boucle, nous voyons que c'est au moment  $n + i$  où on obtient un reste déjà obtenu précédemment au cran  $n$ , ce qui peut s'écrire de la façon suivante :  $10^{n+i} \equiv 10^n \pmod{q}$  ou encore  $10^n(10^i - 1)$  divisible par  $q$ .

Or  $q$  est premier avec 10, on utilise le théorème de Gauss pour conclure que  $(10^i - 1)$  est divisible par  $q$ , ce qui veut dire que l'opération boucle au cran  $i$  et que  $n = 0$ .

Pourquoi une fraction  $\frac{p}{q}$  admet-elle la même valeur de  $n$  et  $i$  que la fraction  $\frac{1}{q}$ ? Si  $p$  est premier avec  $q$ , on a  $p \times 10^n(10^i - 1)$  divisible par  $q$  implique  $10^i - 1$  est divisible par  $q$  et réciproquement. Ceci nous explique pourquoi toutes les familles ont le même nombre d'éléments. A priori, nous disposons d'une théorie complète.

**Récapitulons :** Seules les fractions dont le dénominateur est divisible par 2 ou 5 ont des chiffres avant la période. Le nombre de ces chiffres est égal au plus grand des exposants de 2 ou 5 dans  $q$ . Les fractions  $\frac{p}{q}$  où  $q$  est premier avec 10 sont purement périodiques. Le nombre  $i$  de chiffres de la période ne dépend pas du numérateur et est donné par le plus petit entier  $i$  tel que  $10^i$  soit congru à 1 modulo  $q$ . Les fractions se groupent par familles de  $i$  fractions dont les périodes se déduisent les unes des autres par permutation circulaire.

**Autres exemples**

Pourtant, en quelque sorte, si on veut arriver à une compréhension plus profonde des propriétés en jeu, il semble que notre travail ne fait que commencer. Pour comprendre le texte des *Recherches arithmétiques*, il sera utile de disposer d'autres exemples. Chercher les développements et les familles

<sup>6</sup>c'est-à-dire en prenant le reste dans la division par 13 du nombre obtenu.

de développements pour des dénominateurs de 19 à 29, en appliquant ce que l'on connaît, et donc en effectuant les divisions pour avoir les restes partiels. Nous allons donc nous intéresser aux fractions de dénominateurs 19, 21, 23, 27, 29, (premiers avec 10).

**Fractions  $p/19$  :** On fait le calcul de  $1/19$ , et on trouve une seule famille (restes de 1 à 19).

Q	0, 0 5 2 6 3 1 5 7 8 9 4 7 3 6 8 4 2 1
R	1 10 5 12 6 3 11 15 17 18 9 14 7 13 16 8 4 2 1

**Fractions  $p/21$  :** Il importe de remarquer que les entiers premiers avec 21 forment la liste 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20. Il y a donc 12 fractions irréductibles de dénominateur 21, qui se répartissent en deux familles.

1/21	Q	0, 0 4 7 6 1 9	2/21	Q	0, 0 9 5 2 3 8
	R	1 10 16 13 4 19 1		R	2 20 11 5 8 17 2

Les restes de  $2/21$  sont les doubles des restes de  $1/21$  modulo 21.

**Fractions  $p/23$  :** On fait le calcul de  $1/23$ . Ici encore on obtient une seule famille

1/23	Q	0, 0 4 3 4 7 8 2 6 0 8 6 9
	R	5 6 5 2 1 7 3 9 1 3
	R	1 10 8 11 18 19 6 14 2 20 16 22 13
	R	15 12 5 4 17 9 21 3 7 1

**Fractions  $p/27$  :** On constate qu'il y a 18 fractions irréductibles qui se répartissent en six familles :

1/27	Q	0, 0 3 7
	R	1 10 19 1
2/27	Q	0, 0 7 4
	R	2 20 11 2
4/27	Q	0, 1 4 8
	R	4 13 22 4

5/27	Q	0, 1 8 5
	R	5 23 14 5
7/27	Q	0, 2 5 9
	R	7 16 25 7
8/27	Q	0, 2 9 6
	R	8 26 17 8

**Fractions  $p/29$  :** Ici encore une seule famille; calculons  $1/29$

Q	0 0 3 4 4 8 2 7 5 8 6 2 0 6 8 9
R	6 5 5 1 7 2 4 1 3 7 9 3 1
R	1 10 13 14 24 8 22 17 25 18 6 2 20 26 28 19
R	16 15 5 21 7 12 4 11 23 27 9 3 1

De nombreuses questions sont sous-jacentes aux calculs que nous avons effectués.

Une première question : *peut-on calculer en fonction de  $q$  le nombre de fractions irréductibles de dénominateur  $q$  ?*

Deuxième question : en travaillant sur les restes de divisions, on travaille modulo  $q$  sur les puissances de 10 et l'on voit que pour  $q$  premier avec 10, ces restes sont les nombres premiers avec  $q$ . *Comment travaille-t-on modulo  $q$  ?*

## Les congruences

Nous allons illustrer la théorie des congruences, les résidus de puissances et en particulier la notion de racine primitive<sup>7</sup>. Nous allons introduire par des exemples les théorèmes établis par GAUSS<sup>8</sup>. Ensuite, nous aborderons la compréhension détaillée des tables qu'il a établies et du chapitre six sur les développements décimaux illimités. Nous faisons le choix de rester très près du texte de GAUSS, en gardant, sauf pour une exception que nous expliquons plus loin, sa terminologie et en n'employant pas le langage des structures algébriques. Nous reviendrons là-dessus en conclusion de ce chapitre.

### La théorie des congruences

La notion de congruence est définie dans le premier chapitre, ainsi que les propriétés élémentaires des résidus modulo  $n$ . La suite  $1, 2, \dots, n-1$  est la suite des résidus modulo  $n$ . Chaque entier est congru à un et un seul de ces nombres. Nous utiliserons constamment les résultats suivants :

$$(a \equiv b \text{ et } c \equiv d) \implies (a + c \equiv b + d) \text{ modulo } n$$

$$(a \equiv b \text{ et } c \equiv d) \implies (ac \equiv bd) \text{ modulo } n$$

Le second chapitre est consacré aux congruences du premier degré. Il commence par le théorème dit de GAUSS<sup>9</sup>, l'unique décomposition des entiers en facteurs premiers<sup>10</sup> et ses applications élémentaires<sup>11</sup>. GAUSS traite ensuite la résolution des congruences du premier degré  $ax + by = c$  et les problèmes apparentés<sup>12</sup>.

<sup>7</sup>Là encore, nous pourrions expérimenter pour induire des résultats avant de voir le contenu du livre de GAUSS. Cela donnerait de nombreuses activités.

<sup>8</sup>Chaque énoncé sera suivi de sa référence dans le texte de GAUSS.

<sup>9</sup>paragraphe 14.

<sup>10</sup>paragraphe 16.

<sup>11</sup>paragraphes 17 à 23.

<sup>12</sup>paragraphes 24 à 37.

### Nombre de fractions irréductibles de dénominateur $p$

Cela revient au problème suivant<sup>13</sup> posé par GAUSS :

«Trouver combien il y a de nombres plus petits qu'un nombre donné  $A$  et premiers avec lui?»

Désignons ce nombre par  $\phi(A)$ . GAUSS examine les différents cas :

- Quand  $A$  est un nombre premier  $p$ , il est évident que

$$\phi(p) = p - 1$$

- Quand  $A = p^m$ , pour obtenir  $\phi(A)$  il faut retrancher à  $A$  le nombre d'entiers inférieurs à  $A$  divisible par  $p$ , c'est à dire  $A/p$ , ce qui donne

$$\phi(p^m) = p^m - p^{m-1} = p^m \left(1 - \frac{1}{p}\right)$$

- Quand  $A$  est décomposé en facteurs premiers entre eux  $M \times N \times P \dots$  alors GAUSS montre que

$$\phi(A) = \phi(M) \times \phi(N) \times \phi(P) \times \dots$$

GAUSS applique ensuite cette relation au cas où  $A$  est décomposé en facteurs premiers :

$$A = a^\alpha b^\beta c^\gamma \implies \phi(A) = A \left(1 - \frac{1}{a}\right) \left(1 - \frac{1}{b}\right) \left(1 - \frac{1}{c}\right) \dots$$

**Un exemple pour comprendre :** Cherchons le nombre de fractions irréductibles de dénominateur  $18 = 2 \times 3^2$  : On écrit les nombres de 1 à 18, on enlève les  $18/2$  multiples de 2, on enlève les  $18/3$  multiples de 3, mais on a retiré deux fois les multiples de 6, on doit donc rajouter  $18/6$ .

$$\phi(18) = 18 - \frac{18}{2} - \frac{18}{3} + \frac{18}{6} = 18 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right)$$

Si nous écrivons les 18 fractions de dénominateurs 18, après simplification, elles se répartissent en fractions ayant pour dénominateurs les différents

<sup>13</sup>paragraphe 38.

diviseurs de 18.

$\frac{1}{18}$	$\frac{2}{18}$	$\frac{3}{18}$	$\frac{4}{18}$	$\frac{5}{18}$	$\frac{6}{18}$	$\frac{7}{18}$	$\frac{8}{18}$	$\frac{9}{18}$	$\frac{10}{18}$	$\frac{11}{18}$	$\frac{12}{18}$	$\frac{13}{18}$	$\frac{14}{18}$	$\frac{15}{18}$	$\frac{16}{18}$	$\frac{17}{18}$	$\frac{18}{18}$	
1																		
$\frac{1}{2}$																		
$\frac{1}{3}$						$\frac{2}{3}$												
$\frac{1}{6}$												$\frac{5}{6}$						
$\frac{1}{9}$		$\frac{2}{9}$					$\frac{4}{9}$		$\frac{5}{9}$					$\frac{7}{9}$		$\frac{8}{9}$		
$\frac{1}{18}$					$\frac{5}{18}$	$\frac{7}{18}$					$\frac{11}{18}$	$\frac{13}{18}$						$\frac{17}{18}$

Si on compte les fractions sur chaque ligne<sup>14</sup>, on obtient<sup>15</sup> :

$$18 = \phi(1) + \phi(2) + \phi(3) + \phi(6) + \phi(9) + \phi(18)$$

Nous avons introduit là la *fonction d'Euler* dont GAUSS cite deux articles en référence<sup>16</sup>. GAUSS démontre<sup>17</sup> le résultat que nous avons illustré avec notre tableau :

Si  $a, a', a''$  sont tous les diviseurs de  $A$ <sup>18</sup>, on aura :

$$A = \phi(a) + \phi(a') + \phi(a'') + \dots$$

<sup>14</sup>Cette méthode n'est pas dans le livre de GAUSS, mais elle nous paraît très éclairante.

<sup>15</sup>en posant  $\phi(1) = 1$ .

<sup>16</sup>*Theoremata arithmetica nova methodo demonstrata* comment. nov. acc. Petrop. VIII page 74 et *Speculationes circa quasdam insignes proprietates numerorum* Acta Patrop. VIII p 17.

<sup>17</sup>paragraphe 39.

<sup>18</sup>1 y compris.



### Des résidus des puissances

Dans le chapitre 3, GAUSS étudie les progressions géométriques modulo un entier. Nous disposons déjà de beaucoup d'exemples avec la suite des restes partiels des fractions  $1/q$ , qui sont les suites correspondant aux puissances de 10 modulo  $q$ . Il établit le résultat suivant<sup>19</sup> :

*Dans toute progression géométrique  $1, a, a^2, a^3 \dots$  outre le premier terme 1, il y en a encore un autre  $a^t$  congru à l'unité suivant le module  $p$  premier avec  $a$ , avec l'exposant  $t < p$ .*

Quand on poursuit la progression au delà de l'exposant  $t$ , on obtient une suite périodique. On appelle période la suite de résidus minimum  $1, a, \dots, a^t \dots$  avec l'exposant  $t$  minimum tel que  $a^t$  congru à 1 modulo  $p$ .

Nous allons abandonner la terminologie de GAUSS sur ce seul point et dorénavant nous désignerons par *ordre de  $a$*  cet exposant  $t$ , car c'est ainsi qu'on le désigne actuellement et nous réserverons le mot exposant à son usage habituel. On a toujours  $a^{mt} \equiv 1 \pmod{p}$

$$a^r \equiv a^p \iff r \equiv p \pmod{t}$$

Les  $t$  restes qui composent la période sont tous différents.

#### Résidus de puissances modulo un nombre premier $p$

Nous allons introduire ces notions d'abord sur un exemple que nous allons utiliser plus tard pour expliquer la confection des tables que GAUSS a réalisées.

*Cherchez les ordres des différents résidus modulo 13.*

Cela nous permettra d'expérimenter les calculs sur les puissances modulo 13 et de conjecturer un résultat mathématique. Pour être à l'aise dans ces calculs, il faut utiliser des petits nombres et ne pas hésiter par exemple pour calculer  $9 \times 9$  à utiliser des résidus négatifs comme intermédiaires de calculs :  $9 \times 9 \equiv (-4) \times (-4) \equiv 3$

*Faites vous-mêmes ce calcul avant de poursuivre la lecture.*

<sup>19</sup>paragraphe 45.

#### Puissances modulo 13 :

exposant	1	2	3	4	5	6	7	8	9	10	11	12	ordre
$a = 2$	2	4	8	3	6	12	11	9	5	10	7	1	12
$a = 3$	3	9	1	3	9	1	3	9	1	3	9	1	3
$a = 4$	4	3	12	9	10	1	4	3	12	9	10	1	6
$a = 5$	5	12	8	1	5	12	8	1	5	12	8	1	4
$a = 6$	6	10	8	9	2	12	7	3	5	4	11	1	12
$a = 7$	7	10	5	9	11	12	6	3	8	4	2	1	12
$a = 8$	8	12	5	1	8	12	5	1	8	12	5	1	4
$a = 9$	9	3	1	9	3	1	9	3	1	9	3	1	3
$a = 10$	10	9	12	3	4	1	10	9	12	3	4	1	6
$a = 11$	11	4	5	3	7	12	2	9	8	10	6	1	12
$a = 12$	12	1	12	1	12	1	12	1	12	1	12	1	2

On constate que tous les ordres sont des diviseurs de 12.

*Si  $p$  est un nombre premier qui ne divise pas  $a$ , et que  $a^t$  soit la plus petite puissance de  $a$  congrue à l'unité, l'exposant  $t$  sera  $p - 1$ , ou une partie aliquote<sup>20</sup> de  $p - 1$ <sup>21</sup>.*

GAUSS donne une démonstration de ce théorème qui repose sur une propriété que nous avons déjà rencontrée. Prenons l'exemple des fractions de dénominateurs 27, nous avons trouvé six familles. Écrivons les suites des restes obtenus :

1/27	R	1	10	19	1
2/27	R	2	20	11	2
4/27	R	4	13	22	4

5/27	R	5	23	14	5
7/27	R	7	16	25	7
8/27	R	8	26	17	8

La première suite 1, 10, 19 est la suite correspondant à  $10, 10^2, 10^3$ . GAUSS montre que si cette suite est multipliée par un nombre 2 ne figurant pas dans cette suite, on obtient une suite de nouveaux résidus distincts. Si on prend 4 ne figurant pas dans ces deux suites en multipliant la première suite par 4, on obtient des résidus tous distincts et distincts des précédents etc. Toutes les familles de résidus obtenues ont le même nombre d'éléments. C'est ainsi que GAUSS montre que le nombre d'éléments  $t$  dans la famille  $1, a, a^2, a^3 \dots a^t$  divise  $p - 1$ .

C'est là le théorème<sup>22</sup> dont FERMAT assurait avoir trouvé une démonstration qu'il n'a pas publiée, et dont EULER a fourni deux démonstrations présentées brièvement par GAUSS<sup>23</sup> avec leurs références<sup>24</sup>.

<sup>20</sup>un diviseur de  $p - 1$ .

<sup>21</sup>Théorème 49. On dirait «l'ordre de  $a$  est  $p - 1$  ou un diviseur de  $p - 1$ ».

<sup>22</sup>appelé petit théorème de Fermat.

<sup>23</sup>50.

<sup>24</sup>Fermatii opera math. Tolosae 1679 Fol. p 163 et Démonstration de quelques théorèmes

### Nombre d'entiers ayant un ordre donné

GAUSS désigne par  $\Psi(d)$  le nombre d'entiers ayant pour ordre le nombre  $d$ , modulo le nombre  $p$ . D'après ce que nous venons de voir  $\Psi(d) = 0$  si  $d$  n'est pas un diviseur de  $p$ . Il donne l'exemple  $p = 19$  et remarque que

1 a pour ordre 1	$\Psi(1) = 1,$
18 a pour ordre 2	$\Psi(2) = 1,$
7 et 11 ont pour ordre 3	$\Psi(3) = 2,$
8 et 12 ont pour ordre 6	$\Psi(6) = 2,$
4, 5, 6, 9, 16 et 17 ont pour ordre 9	$\Psi(9) = 6,$
2, 3, 10, 13, 14 et 15 ont pour ordre 18,	$\Psi(18) = 6.$

GAUSS démontre que  $\phi(d) = \Psi(d)$  si  $d$  divise  $p - 1$ , (sinon  $\Psi(d) = 0$ ) pour des congruences modulo un nombre premier. Le lecteur pourra vérifier cette loi pour les ordres  $d$  modulo 13 que nous avons calculés.

### Les racines primitives

Il en déduit qu'il existe toujours des nombres d'ordre maximum  $p - 1$  pour des congruences modulo un nombre premier; il appelle, à la suite d'EULER, *racines primitives*, les valeurs de  $a$  pour lesquelles  $t = p - 1$ . Il a démontré<sup>25</sup> qu'il y en avait  $\phi(p - 1)$  pour des congruences modulo un nombre premier  $p$  et mentionne une erreur d'EULER dans la démonstration de ce résultat car EULER utilise le résultat suivant : la congruence  $x^t - 1$  ne peut avoir plus de  $t$  racines différentes<sup>26</sup>, qui n'est pas vrai pour certains entiers. GAUSS va s'intéresser de façon approfondie aux racines primitives modulo un nombre premier<sup>27</sup>.

Pour  $p = 13$ , ce sont les valeurs 2, 6, 7, 11 pour lesquelles  $t = 12$ .

Pour  $p = 19$ , ce sont les valeurs 2, 3, 10, 13, 14 et 15, pour lesquelles  $t = 18$ .

Dans la première activité sur développements décimaux illimités de rationnels, nous avons montré que lorsque 10 était une racine primitive, les développements formaient une seule famille dont les périodes s'obtenaient à partir de l'une d'elles par permutation circulaire. C'est le cas pour les dénominateurs 7, 17, 19, 23 et 29. La question des racines primitives s'était introduite à propos de ces entiers. GAUSS va montrer comment utiliser d'autres racines primitives que 10 à propos de ces développements décimaux illimités, et comment, si nous connaissons une racine primitive, nous pouvons en

*relatifs aux nombres premiers d'EULER*, en 1736, (Comm. Ac. Petrop. T VIII). GAUSS dément que d'autres mathématiciens avant (LEIBNIZ) aient publié une démonstration.

<sup>25</sup> paragraphes 54 et 55.

<sup>26</sup> paragraphe 56.

<sup>27</sup> paragraphes 49 à 81.

déduire les ordres des différents nombres.

### Théorie des indices

Lorsqu'on a fait le choix d'une racine primitive  $a$ , on appellera indice d'un nombre  $m$  l'exposant  $i$  tel que  $m = a^i$ . On peut remarquer que cet indice est défini modulo  $p - 1$ . En effet, d'après le théorème de Fermat,  $a^{p-1} = 1$ .

Illustrons-le à l'aide de l'exemple  $p = 13$  et faisons le choix de la racine primitive 2. L'indice de  $m$  l'exposant  $i$  de  $m$  tel que  $m = 2^i$ . Faisons un tableau avec pour chaque nombre  $m$  son indice, ce qui consiste à réécrire dans un autre ordre les deux lignes du tableau suivant.

$i$	1	2	3	4	5	6	7	8	9	10	11	12
$m = 2^i$	2	4	8	3	6	12	11	9	5	10	7	1

$m$	1	2	3	4	5	6	7	8	9	10	11	12
indice $i$	12	1	4	2	9	5	11	3	8	10	7	6

Ce tableau signifie par exemple  $a = 5 = 2^9$ , on en déduit que l'exposant de 5 est 4, plus petit entier qui multiplié par 9 donne un multiple de 12.

On peut en déduire aussi que tous les nombres  $a$  dont l'indice est un nombre premier avec 12 sont aussi racines primitives. Si donc il y a une racine primitive modulo  $p$ , il y en a  $\phi(p - 1)$ .

### Un logarithme

Tout résidu modulo  $p$ , si  $a$  est une racine primitive, est caractérisé par son exposant dans la base  $a$ , exposant que GAUSS, à la suite d'EULER appelle son indice. GAUSS développe une théorie des indices analogue à celle des logarithmes. Une fois choisie une racine primitive modulo  $p$ , il montre :

*L'indice d'un produit de tant de facteurs qu'on voudra, est congru à la somme des indices des différents facteurs, suivant le module  $p-1$ .*<sup>28</sup>

*L'indice de la puissance  $n^r$  d'un nombre est congru, suivant le module  $p-1$ , au produit de l'exposant  $r$  par l'indice du nombre  $n$  donné.*

GAUSS établit les relations entre les indices d'un nombre quand on change de racine primitive. Son problème, pour établir sa première table d'indices est de trouver une racine primitive. Comme il le dit lui-même<sup>29</sup>

<sup>28</sup> paragraphe 58.

<sup>29</sup> paragraphe 73.

La plupart des méthodes qui servent à trouver les racines primitives reposent en grande partie sur le tâtonnement.

GAUSS construit une première table, où pour chaque entier  $q$ , premier ou puissance d'un nombre premier, possédant une racine primitive, il fait figurer pour chaque nombre premier  $p$ , son indice. Avec la décomposition des nombres en facteurs premiers, ceci permet de calculer pour tout nombre  $n$  l'indice de ce nombre, modulo  $\phi(q)$ .

Quand il y a plusieurs choix possibles de racines primitives, GAUSS choisit pour  $a$  celle où 10 a un indice minimum<sup>30</sup>. Quand 10 est racine primitive, c'est donc 10 qui est choisi comme base des indices. Quand on consulte la table pour le nombre 13, on constate que GAUSS a choisi pour racine primitive non pas la plus petite 2, mais la racine primitive 6.

### Racine primitives modulo un nombre composé

La question des racines primitives est considérée par EULER comme une des questions les plus difficiles en arithmétique. GAUSS cherche des conditions d'existence pour des racines primitives modulo un nombre composé<sup>31</sup>.

Précisons sur l'exemple  $n = 18$  les phénomènes qui se passent. Il y a parmi les nombres plus petits que 18 des nombres qui sont diviseurs de zéro modulo 18. Nous allons distinguer les résidus 1, 5, 7, 11, 13, 17 premiers avec 18; Il y en a  $\phi(18) = 6$ . Le produit de deux tels résidus est encore un résidu premier avec 18. Voici la table de multiplication de ces résidus modulo 18 :

mod18	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	5	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Si  $f$  désigne combien il y a de nombres premiers avec  $m$  et moindres que lui, c'est-à-dire si  $f = \phi(m)$ , l'exposant  $t$  de la plus petite puissance d'un nombre donné  $a$ <sup>32</sup> premier avec  $m$ , qui est congrue à l'unité suivant le module  $m$  sera égal à  $f$  ou une partie aliquote de  $f$ .<sup>33</sup>

<sup>30</sup>paragraphe 72.

<sup>31</sup>à partir du paragraphe 82.

<sup>32</sup>l'ordre de  $a$ .

<sup>33</sup>paragraphe 83. C'est le théorème d'EULER (1760); curieusement GAUSS cite ce résultat sans faire référence à EULER.

La démonstration du théorème d'EULER est facile à illustrer à l'aide du tableau précédent. Désignons par  $P = 1 \times 5 \times 7 \times 11 \times 13 \times 17$  le produit de tous les résidus que l'on retrouve sur chaque ligne. Prenons la ligne  $a$ . Nous trouvons sur cette ligne le produit par  $a$  de chacun des résidus précédents. Cela montre que

$$P = (a \times 1) \times (a \times 5) \times (a \times 7) \times (a \times 11) \times (a \times 13) \times (a \times 17) = a^{\phi(18)} P$$

On en déduit, pour tout nombre  $a$  premier avec 18 :

$$a^{\phi(18)} = 1$$

GAUSS démontre ensuite qu'il y a des racines primitives pour des nombres du type  $p^n$ ,  $p$  étant un nombre premier impair<sup>34</sup>. Il démontre le résultat suivant :

*Si le plus grand diviseur de  $t$  et de  $p^{n-1}(p-1)$  est  $e$ , la congruence  $x^t - 1$  modulo  $p^n$  aura  $e$  racines différentes.*

Il en déduit l'existence de racines primitives pour les nombres<sup>35</sup> du type  $p^n$  pour  $p \neq 2$ .

Afin d'illustrer les phénomènes qui se passent, nous pouvons examiner les cas de 8 et d'entiers qui ne sont pas une puissance d'un nombre premier impair. Examinons les cas  $p = 8$ ,  $p = 12$  et  $p = 15$ .

**Puissances modulo 8 :** Pour  $p = 8$ , on calcule les puissances de 4 nombres : 1, 3, 5, 7. Tous les résidus vérifient l'équation  $x^2 - 1 = 0$  qui a donc plus de deux racines.

exposant	1	2	3	4	ordre
$a = 1$	1	1	1	1	1
$a = 3$	3	1	3	1	2
$a = 5$	5	1	5	1	2
$a = 7$	7	1	7	1	2

**Puissances modulo 12 :** Pour  $p = 12$ , on calcule les puissances de 4 nombres : 1, 5, 7, 11. Tous les résidus vérifient l'équation  $x^2 - 1 = 0$  qui a donc plus de deux racines.

exposant	1	2	3	4	ordre
$a = 1$	1	1	1	1	1
$a = 5$	5	1	5	1	2
$a = 7$	7	1	7	1	2
$a = 11$	11	1	11	1	2

<sup>34</sup>La démonstration faite dans le cas d'un entier premier utilisait le résultat suivant qui ne se généralise pas : le congruence  $x^t - 1$  ne peut avoir plus de  $t$  racines différentes.

<sup>35</sup>paragraphe 88 et 89.

**Puissances modulo 15 :** Pour  $p = 15$ , on calcule les puissances de 8 nombres : 1, 2, 4, 7, 8, 11, 13, 14 : Tous les résidus vérifient l'équation  $x^4 - 1 = 0$  qui a donc plus de quatre racines.

exposant	1	2	3	4	5	6	7	8	ordre
$a = 1$	1	1	1	1	1	1	1	1	1
$a = 2$	2	4	8	1	2	4	8	1	4
$a = 4$	4	1	4	1	4	1	4	1	2
$a = 7$	7	4	13	1	7	4	13	1	4
$a = 8$	8	4	2	1	8	4	2	1	4
$a = 11$	11	1	11	1	11	1	11	1	2
$a = 13$	13	4	7	1	13	4	7	1	4
$a = 14$	14	1	14	1	14	1	14	1	2

GAUSS démontre que pour les nombres modulo  $2^n$  pour  $n > 2$ , la puissance  $2^{n-2}$  de tout nombre impair  $y$ <sup>36</sup> est égale à 1, et donc qu'il n'y a pas de racines primitives. Il démontre ensuite qu'il n'y a pas de racines primitives modulo un nombre composé de plusieurs nombres premiers sauf pour les entiers  $2 \times p^n$ .

**Il existe des racines primitives seulement pour les entiers  $m = 2$ ,  $m = 4$ ,  $m = p^n$ ,  $m = 2 \times p^n$ , avec  $p$  premier impair.**<sup>37</sup>

GAUSS annonce à la fin du chapitre trois, qu'il va pouvoir se passer de l'usage des racines primitives dans le cas de modules composés, en décomposant une congruence modulo  $n$  en une série de congruences modulo des  $p^m$ . Il donne comme référence deux articles d'EULER<sup>38</sup> sur ces questions.

Nous utiliserons la table qu'il a établie en annexe au troisième chapitre, pour calculer les indices des entiers jusqu'à 100 modulo une racine primitive et voir l'application de cette théorie aux développements illimités de rationnels. Mais avant, donnons quelques indications historiques ultérieures.

### Développements ultérieurs

Cette question des racines primitives a été beaucoup étudiée après EULER et GAUSS. Des tables de racines primitives ont été établies, par exemple par

<sup>36</sup> paragraphe 90.

<sup>37</sup> paragraphe 92.

<sup>38</sup> *Theoremata circa residua ex divisione potestatum relicta* (comm. nov. Petrop. T. VII p 49) et *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia* (ibid. T XVIII p. 85).

JACOBI en 1839 pour tous les entiers premiers jusqu'à 1000, par CUNNINGHAM en 1900, pour les entiers premiers jusqu'à 10000 et la course ne s'est pas arrêtée là... On trouve une étude historique très complète sur les racines primitives et les congruences dans le deuxième chapitre du livre de DICKSON sur l'histoire de la théorie des nombres<sup>39</sup>.

### Développements décimaux illimités de rationnels

Revenons sur ces développements pour comprendre la préoccupation de GAUSS. À l'époque où il a fait ce travail, aucun de nos moyens de calculs actuels n'était disponible. La préoccupation de GAUSS était de fournir une table avec le minimum de renseignements qui permette d'obtenir facilement le développement illimité de n'importe quel rationnel. C'est à cela que va servir sa théorie de l'indice.

#### Se ramener à des dénominateurs $p^n$

GAUSS montre qu'on peut décomposer toute fraction  $\frac{m}{n}$  irréductible où  $n = a \times b$  avec  $a$  et  $b$  étant deux entiers premiers entre eux à une somme de deux fractions irréductibles de dénominateurs  $a$  et  $b$ <sup>40</sup>.

$$\frac{m}{n} = \frac{m_1}{a} + \frac{m_2}{b}$$

Il en déduit que toute fraction peut s'écrire, si son dénominateur a pour décomposition en facteurs premiers  $n = a^\alpha \times b^\beta \times c^\gamma \dots$  de façon unique sous la forme d'une somme d'un entier et de fractions<sup>41</sup> plus petites que 1 :

$$k + \frac{m_1}{a^\alpha} + \frac{m_2}{b^\beta} + \frac{m_3}{c^\gamma} \dots$$

Pour trouver le développement décimal illimité de  $\frac{m}{n}$ , il suffit donc de connaître celui de chacune des fractions du second membre, c'est-à-dire celui des fractions dont le dénominateur est une puissance d'un nombre premier. D'après l'étude faite en première partie, les puissances de 2 et de 5 interviennent pour fournir les chiffres avant la période. En utilisant les transformations que nous avons expliquées dans la première partie, nous voyons que nous pouvons supposer que les dénominateurs sont de la forme  $p^n$  avec  $p$  nombre premier impair, distinct de 5 et donc premier avec 10.

<sup>39</sup> DICKSON *History of the theory of numbers*.

<sup>40</sup> paragraphe 309.

<sup>41</sup> paragraphe 310.

### Fractions de dénominateurs $p^n$

Nous avons vu que le développement des fractions  $\frac{10 \times m}{p^n}, \frac{10^2 \times m}{p^n} \dots \frac{10^e \times m}{p^n}$  s'obtiennent à partir du développement de  $\frac{m}{p^n}$  en supprimant 1, 2...e chiffres juste après la virgule, lorsque e est la plus petite puissance de 10 congrue à l'unité modulo  $p^n$ . Lorsque nous connaissons le premier développement, si nous savons quel décalage effectuer, nous connaissons e développements.

#### Cas où 10 est racine primitive

Examinons le cas où  $p = 17$ . GAUSS dans sa table d'indices fournit les résultats suivants où 10 est la racine primitive utilisée :

premiers	2	3	5	7	11	13
indices	10	11	7	9	13	12

D'autre part dans la troisième table des développements nous trouvons un seul développement :

$$(0) \dots\dots\dots 0588235294117647$$

Cherchons le développement de  $\frac{16}{17}$ . Pour cela nous allons calculer l'indice de  $16 = 2^4$ . L'indice est donc  $40 \equiv 8$  modulo  $p - 1 = 16$ . On a donc  $16 \equiv 10^8$  modulo 17. Le développement de  $\frac{16}{17}$  s'obtient donc en supprimant huit chiffres après la virgule dans celui de  $\frac{1}{17}$ . On obtient donc

$$\frac{16}{17} = 0, \overline{9411764705882352}$$

#### Cas où 10 n'est pas racine primitive

Nous savons que nous avons plusieurs familles de développements. Pour calculer le développement d'une fraction, nous devons déterminer à quelle famille elle appartient, puis quel décalage nous devons effectuer. Ici encore nous allons nous servir des deux tables de GAUSS sur les deux exemples que nous avons étudiés en détail dans la première partie à savoir les dénominateurs 13 et  $27 = 3^3$ .

#### Cas $p = 13$

GAUSS a fait le choix de la racine primitive 6 où l'indice de 10 était minimum. D'après l'étude faite en deuxième partie, il y a  $\phi(13) = 12$  développements répartis en deux familles puisque  $10^6 \equiv 1$  modulo 13. Rappelons que les calculs d'indices s'effectuent modulo 12.

premiers	2	3	5	7	11
indices	5	8	9	7	11

L'indice de 10 est  $14 \equiv 2$  modulo 12 et est effectivement minimum pour cette racine primitive 6.

Dans la table des développements, nous trouvons deux développements écrits de la façon suivante.

$$(0) \dots 076923 ; (1) \dots 461538$$

Ces deux développements sont ceux des fractions  $\frac{1}{13}$  et  $\frac{6}{13}$ , car 6 est la racine primitive.

Cherchons les développements des deux fractions  $\frac{11}{13}$  et  $\frac{12}{13}$ . Il nous faut savoir à quelle famille appartient chaque fraction et quel décalage effectuer. Pour cela nous allons chercher les indices de 11 et 12, modulo 12.

L'indice de 11 se lit sur la table. Il est égal à 11. Or  $11 = 2 \times 5 + 1$ , c'est-à-dire  $11 \equiv 6^{11}$  et  $11 \equiv 6^{2 \times 5} \times 6^1$  modulo 13; or  $6^2 = 10$  donc  $11 \equiv 10^5 \times 6$ . La fraction  $\frac{11}{13}$  appartient à la famille de la fraction  $\frac{6}{13}$  et on obtient son développement en effectuant un décalage de 5

$$\frac{11}{13} = 0, \overline{846153}$$

L'indice de 12 se calcule à partir des indices de 2 et 3. Il est égal à 18, donc à 6 modulo 12. Or  $6 = 2 \times 3$ , c'est-à-dire  $12 \equiv 6^{2 \times 3}$ ,  $12 \equiv 6^{2 \times 3}$  modulo 13, ou encore  $12 \equiv 10^3$ . La fraction  $\frac{12}{13}$  appartient à la famille de la fraction  $\frac{1}{13}$  et on obtient son développement en effectuant un décalage de 3

$$\frac{12}{13} = 0, \overline{923076}$$

#### Cas $p = 27$

Le tableau des indices est le suivant, en utilisant 2 comme racine primitive.

premiers	2	3	5	7	11	13	17	19	23
indices	1	$\times$	5	16	13	8	15	12	11

Ici nous savons qu'il y a  $\phi(27) = 18$  fractions irréductibles réparties en 6 familles, puisque l'ordre de 10 est 3, et son indice est 6. Les calculs d'indices se font modulo  $\phi(18) = 6$ .

Pour déterminer les familles, GAUSS place dans sa table trois les développements des fractions :

$$(0) \dots 037 ; (1) \dots 074 ; (2) \dots 148 ; (3) \dots 296 ; (4) \dots 592 ; (5) \dots 185$$

Ces développements correspondent aux fractions  $\frac{1}{27}, \frac{2}{27}, \frac{4}{27}, \frac{8}{27}, \frac{16}{27}, \frac{5}{27}$ .

Pour trouver le développement décimal illimité d'une fraction quelconque, il faut calculer l'indice du numérateur pour voir dans quelle famille se trouve la fraction et quel décalage effectuer.

Prenons par exemple la fraction  $\frac{17}{27}$ . L'indice du numérateur 17 est 15. Or  $15 = 6 \times 2 + 3$  et  $2^{15} = 10^2 \times 2^3$ . La fraction appartient à la troisième famille et on doit faire un décalage de 2. On obtient donc :

$$\frac{17}{27} = 0, \overline{629}$$

**Résultats généraux :** Dans le cas d'un dénominateur  $p^\mu$ , si  $10^e \equiv 1$  modulo  $p^\mu$ , il y a  $\phi(p^\mu) = p^{\mu-1}(p-1) = ef$  fractions irréductibles.

GAUSS a choisi une racine primitive  $a$  telle que 10 ait pour indice  $f$ . Il avait montré que cela était toujours possible<sup>42</sup> et GAUSS fait figurer dans sa table de développements, les développements des fractions  $\frac{1}{p^\mu}, \frac{a}{p^\mu}, \frac{a^2}{p^\mu}, \frac{a^3}{p^\mu}, \dots, \frac{a^{f-1}}{p^\mu}$ .

Pour savoir quel est le développement de la fraction  $\frac{b}{p^\mu}$ , on calcule l'indice  $i$  de  $b$ , on fait la division euclidienne de  $i$  par  $f$ . Si on a  $i = cf + r$  alors la fraction  $\frac{b}{p^\mu}$  appartient à la famille  $\frac{a^r}{p^\mu}$  et s'obtient en faisant un décalage de  $c$  places dans cette famille<sup>43</sup>.

### Conclusion

Dans ce chapitre, nous avons exposé la théorie des congruences telle qu'elle figure dans GAUSS, sans utiliser du tout le langage des structures algébriques. Nous pensons que cela peut aussi être une étape dans l'enseignement où au lieu d'utiliser la formalisation la plus récente, on fait les démonstrations dans le langage des congruences, avant de parler de groupes finis.

Toute cette théorie n'est pas une curiosité historique et les idées développées dans ce chapitre sont très importantes dans les théories du codage. Bien sûr, la théorie des développements décimaux n'est pas centrale dans les recherches mathématiques actuelles. Elle a eu l'avantage de nous faire aborder ces questions d'une façon simple et naturelle.

### Documentation

DEMAZURE. Cours d'algèbre, primalité, divisibilité, codes. Éditions Cassini 1997.

<sup>42</sup>paragraphe 71.

<sup>43</sup>paragraphe 315.

DICKSON. History of numbers. Chelsea publishing company.

DE KONINCK ET MERCIER. Introduction à la théorie des nombres. collection Modulo 1994.

GAUSS. Disquisitiones arithmeticae. réédition Blanchard 1979.

OYSTEIN ORE. Number theory and its history. Éditions Dover (1988) réédition d'un livre de 1948.

## SECTION SIXIÈME.

*Applications des différentes Recherches précédentes.*

508. Nous avons déjà indiqué en différens endroits combien l'arithmétique transcendante peut être utile dans les autres parties des mathématiques. Mais nous ne croyons pas inutile de traiter à part quelques applications qui méritent d'être exposées avec plus de détail, non dans la vue d'épuiser ce sujet, qui suffirait pour remplir plusieurs volumes, mais pour l'éclaircir par quelques exemples.

Dans cette Section, nous parlerons d'abord de la décomposition des fractions en fractions plus simples; ensuite, de la conversion des fractions ordinaires en fractions décimales; nous exposerons une nouvelle méthode d'exclusion, qui sert à la résolution des équations indéterminées du second degré; enfin, nous donnerons de nouvelles méthodes abrégées, pour distinguer les nombres premiers des nombres composés, et trouver les facteurs de ces derniers.

312. *Définition.* Si l'on convertit une fraction ordinaire en fraction décimale, la suite de figures décimales (\*) (en excluant la partie entière, s'il y en a), soit finie, soit infinie, s'appellera *mantisse* de la fraction, en prenant ici dans une acception plus générale une expression qui n'était jusqu'à présent usitée que pour les logarithmes. Ainsi, par exemple, la mantisse de la fraction  $\frac{1}{2}$  est 125, la mantisse de la fraction  $\frac{3}{2}$  est 1875, celle de la fraction  $\frac{1}{3}$  est 054954..... à l'infini.

Il suit de là sur-le-champ, que deux fractions  $\frac{l}{n}$  et  $\frac{m}{n}$  de même) ---

(\*) Pour abrégér, nous ne nous arrêtons qu'au système décimal vulgaire quoique nos recherches pussent s'étendre à un système quelconque.

## RECHERCHES

nous ferons voir ensuite comment on peut y ramener les autres. Nous commencerons par observer que la mantisse d'une telle fraction  $\frac{a}{p^\mu}$ , dans laquelle nous supposons que le numérateur  $a$  ne soit pas divisible par le nombre premier  $p$ , est toujours finie lorsque  $p=2$ , ou  $=5$ , et qu'elle est composée de  $\mu$  chiffres. Dans le premier cas, cette mantisse, considérée comme un nombre entier, sera  $5^\mu a$ ; dans le second,  $2^\mu a$ . Ces vérités sont si évidentes, qu'il est inutile de s'y arrêter.

Mais si  $p$  est un autre nombre premier,  $10^a$  ne sera jamais divisible par  $p^\mu$ , quel que grand que l'on prenne  $r$ , d'où il suit que la mantisse de la fraction  $F = \frac{a}{p^\mu}$  est nécessairement infinie. Supposons que  $10^r$  soit la plus petite puissance de 10 qui soit congrue à l'unité, suivant le module  $p^\mu$  (V. Section III, où nous avons fait voir que  $e$  est égal à  $(p-1)^{p^{\mu-1}}$ , ou à une partie aliquote de ce nombre), on voit facilement que  $10^r a$  est le premier nombre de la suite  $10a, 100a, 1000a, \dots$ , etc. qui soit congru avec  $a$ , suivant le même module. Or comme, par le n° 312, les mantisses des fractions  $\frac{10a}{p^\mu}, \frac{100a}{p^\mu}, \frac{1000a}{p^\mu}, \dots, \frac{10^r a}{p^\mu}$  résultent de celle de la fraction  $F$  en supprimant le premier chiffre, les deux, trois, etc.  $e$  premiers chiffres, il est évident que dans cette mantisse, après les  $e$  premiers chiffres, et non auparavant, les mêmes chiffres reparaitront dans le même ordre. Ces  $e$  premiers chiffres qui, répétés à l'infini, forment la mantisse, peuvent être nommés *période* de cette mantisse ou de la fraction, et il est clair que la grandeur de la période, c'est-à-dire le nombre des chiffres qui la composent, qui est  $=e$ , est tout-à-fait indépendant du numérateur  $a$ , et que le dénominateur seule détermine. Ainsi, par exemple, la période de la fraction  $\frac{1}{7}$  est 09, celle de la fraction  $\frac{2}{7}$  est 428571 (\*).

(\*) Robertson marque le commencement et la fin de la période, en plaçant un point sur le premier et le dernier chiffre (*Theory of circulating fractions, Philos. trans., 1764*), mais nous ne l'avons pas jugé nécessaire.

dénominateur ont des mantisses égales ou différentes, suivant que les numérateurs  $l, m$  sont congrus ou incongrus suivant  $n$ . Une mantisse finie ne change pas lorsqu'on ajoute plusieurs zéros à sa droite. La mantisse de la fraction  $\frac{10^m}{n}$  s'obtient en retranchant la première figure de la mantisse de la fraction  $\frac{m}{n}$ , et généralement, la mantisse de la fraction  $\frac{10^m}{n}$  se trouve en retranchant les  $\nu$  premières figures de la mantisse de la fraction  $\frac{m}{n}$ . La mantisse de la fraction  $\frac{1}{n}$  commence par un chiffre significatif, si  $n < 10$  ou  $= 10$ ; mais si  $n > 10$ , et que le nombre de ses chiffres soit  $k$ , les  $k-1$  premières figures de la mantisse seront des zéros, et la  $k^{\text{ième}}$  un chiffre significatif. Il suit de là que si  $\frac{l}{n}$  et  $\frac{m}{n}$  ont des mantisses différentes, c'est-à-dire, si  $l$  et  $m$  sont incongrus suivant  $n$ , ces mantisses ne peuvent avoir les  $k$  premiers chiffres égaux, et qu'elles diffèrent au moins dans le  $k^{\text{ième}}$ .

313. PROBLÈME. *Etant donné le dénominateur d'une fraction  $\frac{m}{n}$ , et les  $k$  premières figures de sa mantisse, trouver le numérateur  $m$ , que nous supposons plus petit que  $n$ .*

Considérons ces  $k$  figures comme un nombre entier; multiplions-le par  $n$  et divisons le produit par  $10^k$ , en en retranchant les  $k$  premières figures; si le quotient est entier, c'est-à-dire, si les chiffres retranchés sont des zéros, ce sera évidemment le numérateur cherché, et la mantisse donnée sera complète, sinon le numérateur cherché sera l'entier immédiatement plus grand, ou ce quotient augmenté de l'unité, lorsqu'on en aura retranché la partie décimale. La raison de cette règle se tire si facilement des observations que nous avons faites à la fin du n° précédent, qu'il n'y a pas besoin de plus grands développemens.

*Exemple.* Si l'on sait que 69 sont les deux premières figures de la mantisse de la fraction dont le dénominateur est 23. on a le produit  $23.69 = 1587$ ; retranchant les deux derniers chiffres, et ajoutant l'unité, on trouve 16 pour le numérateur cherché.

314. Considérons d'abord les fractions dont les dénominateurs sont des nombres premiers ou des puissances de nombres premiers;

## ARITHMÉTIQUES.

315. Ainsi, dès que l'on connaît la période d'une fraction, on peut obtenir la mantisse avec autant de figures qu'on voudra; d'ailleurs il est clair que si l'on a  $b \equiv 10^a \pmod{p^\mu}$ , on obtient la période de la fraction  $\frac{b}{p^\mu}$ , si (en supposant, comme il est toujours permis, que  $\lambda < e$ ) on écrit les  $\lambda$  premiers chiffres de la période de la fraction  $F$  après les  $e-\lambda$  qui restent, et par conséquent lorsqu'on a la période de la fraction  $F$ , on a en même temps celles de toutes les fractions dont les numérateurs sont congrus aux nombres  $10a, 100a, 1000a, \dots$ , suivant le module  $p^\mu$ . Ainsi, par exemple, comme  $6 \equiv 3.10 \pmod{7}$ , la période de la fraction  $\frac{6}{7}$  se trouve au moyen de la période de la fraction  $\frac{3}{7}$ ; elle est 857142.

Donc toutes les fois que, pour le module  $p^\mu$ , le nombre 10 est une racine primitive (nos 57 et 89), on peut, de la période de la fraction  $\frac{1}{p^\mu}$ , déduire sur-le-champ la période de toute autre fraction  $\frac{m}{p^\mu}$ ,  $m$  n'étant pas divisible par  $p$ , en retranchant à gauche pour écrire à droite, autant de chiffres qu'il y a d'unités dans l'indice du nombre  $m$ , 10 étant pris pour base. On voit par là pourquoi, dans la Table I, nous avons toujours pris 10 pour base, quand la chose était possible.

Mais quand 10 n'est pas racine primitive, on ne peut tirer de la période de la fraction  $\frac{1}{p^\mu}$  que celles des fractions dont les dénominateurs sont congrus, suivant  $p^\mu$ , à quelque puissance de 10. Soit  $10^r$  la plus petite puissance de 10 congrue à l'unité, suivant le module  $p^\mu$ , faisons  $(p-1)^{p^{\mu-1}} = ef$ , et prenons (n° 71) pour base une racine primitive  $r$  telle que  $f$  soit l'indice du nombre 10. Dans ce système, les numérateurs des fractions dont les périodes peuvent se tirer de la période de la fraction  $\frac{1}{p^\mu}$ , auront pour indices

$$f, 2f, 3f, \dots, (e-1)f.$$

De la même manière, on peut déduire de la période de la fraction  $\frac{1}{p^m}$ , celles des fractions dont les numérateurs répondent aux indices

$$f+1, 2f+1, 3f+1, \text{ etc.}$$

De la période de la fraction dont le numérateur est  $r^a$  (l'indice en est 2), on déduira celles des fractions dont les numérateurs ont pour indices

$$f+2, 2f+2, 3f+2, \text{ etc.}$$

Et généralement, de la période de la fraction dont le numérateur est  $r^i$ , on déduira celles des fractions dont les numérateurs ont pour indices

$$f+i, 2f+i, 3f+i, \text{ etc.}$$

On conclura facilement de là que si l'on connaît seulement les périodes des fractions qui ont pour numérateurs

$$1, r, r^2, r^3, \dots, r^{f-1},$$

on peut tirer toutes les autres par la seule transposition, à l'aide de la règle suivante : Soit  $i$  l'indice du numérateur  $m$  de la fraction proposée  $\frac{m}{p^k}$ , dans le système où  $r$  est pris pour base, nous

supposons  $i < (p-1)p^{m-1}$ ; on fera, en divisant par  $f$ ,  $i = \alpha f + \beta$ , de manière que  $\alpha, \beta$  soient des entiers positifs, ou même  $= 0$ , et qu'on ait  $\beta < f$ . Cela posé, la période de la fraction  $\frac{m}{p^k}$  naîtra

de celle de la fraction dont le numérateur est  $r^\beta$  (et partant 1, quand  $\beta = 0$ ) en plaçant les  $\alpha$  premiers chiffres après les autres (et conservant par conséquent cette période elle-même, quand  $\alpha = 0$ ). Ce qui précède suffit pour faire voir pourquoi, en formant la Table I, nous avons suivi la règle exposée n° 72.

516. Nous avons construit, d'après ces principes, pour tous les dénominateurs de la forme  $p^k$ , au-dessous de 1000, une Table des périodes nécessaires, que nous donnerons en entier, et même continuée plus loin à la première occasion qui se présentera. Nous

et l'on trouve 8490566037735 pour la période cherchée. Les chiffres initiaux 84 sont dans ce cas séparés dans la Table.

Nous observerons encore, qu'à l'aide de la Table III on peut trouver un nombre qui, pour un module donné, contenu dans cette Table, dans la colonne des dénominateurs, répond à un indice donné, ainsi que nous l'avons promis n° 59: il suit en effet de ce que nous avons dit plus haut, que l'on peut trouver la période d'une fraction au numérateur de laquelle répond un indice donné, quoique ce numérateur soit inconnu; il suffit de prendre de cette période autant de chiffres initiaux qu'il y a de chiffres au dénominateur, et par le n° 313, on trouvera, à l'aide de ces chiffres, le numérateur, ou le nombre cherché qui répond à l'indice donné.

317. On peut par ce qui précède trouver sans calcul la mantisse d'une fraction quelconque, dont le dénominateur est un nombre premier, ou une puissance d'un nombre premier compris entre les limites de la Table. Mais, à l'aide des recherches que nous avons faites au commencement de cette Section, l'usage de cette Table devient bien plus étendu, et elle renferme même les fractions dont les dénominateurs sont des produits de nombres premiers ou de puissances de nombres premiers. En effet, une pareille fraction peut se décomposer en d'autres dont les dénominateurs soient ces facteurs, et ces dernières peuvent être converties en fractions décimales, avec tel degré d'approximation qu'on voudra; ainsi il ne reste qu'à les réunir par l'addition. Il est à peine nécessaire d'observer que le dernier chiffre de la somme pourra se trouver un peu plus petit qu'il ne devrait être; mais il est évident que l'erreur ne peut monter à autant d'unités qu'il y a de fractions à ajouter; ainsi il conviendrait de calculer ces dernières avec quelques figures de plus qu'on n'en veut avoir à la fraction proposée.

Considérons, comme exemple, la fraction

$$F = \frac{60938031}{117180710} (*),$$

(\*) Cette fraction est une de celles qui approchent le plus de la racine carrée de 23, et l'excès est moindre que sept unités du vingtième ordre décimal.

plaçons ici la Table III, pour en donner une idée; elle ne va que jusqu'à 100, et elle a à peine besoin d'explication.

Pour les dénominateurs à l'égard desquels 10 est racine primitive, elle donne les périodes des fractions dont le numérateur est 1, par exemple pour les nombres:

$$7, 17, 19, 23, 29, 47, 59, 61, 97;$$

pour les autres, les  $f$  périodes qui répondent aux numérateurs 1,  $r$ ,  $r^2, \dots, r^{f-1}$ , périodes qui sont distinguées par les nombres (0), (1), (2), etc.; on a toujours pris la même base que dans la Table I. A l'aide de cette Table et de ce qui a été enseigné dans le n° précédent, on peut trouver la période d'une fraction quelconque, pourvu que son dénominateur soit contenu dans cette Table, et que l'on ait calculé l'indice du numérateur au moyen de la Table I. Au reste, pour des dénominateurs aussi petits, on peut se passer de la Table I, en calculant par la division arithmétique autant de chiffres de la mantisse cherchée, qu'il est nécessaire, d'après le n° 313, pour la distinguer de toute autre du même dénominateur (pour la Table III, il n'en faut jamais plus de deux), et en parcourant les différentes périodes qui répondent au dénominateur donné, jusqu'à ce que nous soyons parvenus à ces chiffres initiaux, qui indiqueront sûrement le commencement de la période. Il faut cependant avertir que ces chiffres peuvent être séparés de manière que le premier, ou plusieurs, forment la fin de la période, et l'autre ou les autres la commencement.

Exemple. On demande la période de la fraction  $\frac{1}{12}$ . La Table I donne, pour la base 19, ind. 12 = 2. ind. 2 + ind. 3 = 39 ≡ 3 (mod. 18) (n° 57). Donc, comme dans ce cas il n'y a qu'une seule période qui répond au numérateur, il faut transporter à la fin les trois premiers chiffres, ce qui donne 631578947368421052. Les deux premiers chiffres 63 avaient fait trouver aussi facilement le commencement de la période.

Si l'on demande la période de la fraction  $\frac{5}{13}$ , on trouve pour le module 53, ind. 45 = 2 ind. 5 + ind. 5 = 49; le nombre des périodes est ici, 4 =  $f$ , et l'on a 49 = 12 $f$  + 1; donc il faut à la période désignée par (1) transposer les douze premiers chiffres,

dont le dénominateur est le produit des nombres 16, 9, 5, 49, 13, 47, 59. On trouve par ce qui précède

$$F = 1 + \frac{1}{16} + \frac{1}{9} + \frac{1}{5} + \frac{1}{13} + \frac{1}{49} + \frac{1}{13} + \frac{1}{7} + \frac{1}{53};$$

ces fractions particulières réduites en décimales, donnent

$$\begin{array}{l} 1 = 1 \\ \frac{1}{16} = 0,6875 \\ \frac{1}{9} = 0,8 \\ \frac{1}{5} = 0,4444444444 \\ \frac{1}{13} = 0,4444444444 \\ \frac{1}{49} = 0,4444444444 \\ \frac{1}{13} = 0,4444444444 \\ \frac{1}{7} = 0,4444444444 \\ \frac{1}{53} = 0,3840153846 \\ \frac{1}{49} = 0,1489561702 \\ \frac{1}{53} = 0,8813559322 \\ F = 4,7958315233 \end{array} \quad \begin{array}{l} 4444444444 \\ 4444444444 \\ 4444444444 \\ 4444444444 \\ 4444444444 \\ 4444444444 \\ 4444444444 \\ 1538461538 \\ 1276595744 \\ 0358983050 \\ 1271954166 \end{array} \quad \begin{array}{l} 44 \\ 75 \\ 46 \\ 68 \\ 84 \\ 17. \end{array}$$

L'erreur en moins de cette somme, comparée, à la valeur exacte; est moindre que cinq unités du vingt-deuxième ordre, donc les vingt premiers chiffres sont exacts. En poussant le calcul à un plus grand nombre de décimales, au lieu des deux derniers chiffres 17, on trouve 1893936. Au reste, chacun sentira bien, même sans que nous en avertissions, que cette méthode de réduire les fractions ordinaires en fractions décimales, est principalement applicable au cas où l'on veut avoir un grand nombre de chiffres; car, s'il suffit d'un petit nombre, la division ou les logarithmes peuvent être souvent employés avec autant d'avantage.

318. Comme nous avons ramené les fractions dont le dénominateur est composé de plusieurs nombres premiers différents, au cas où le dénominateur est un nombre premier, ou une puissance d'un nombre premier, il ne nous reste qu'à ajouter quelque chose sur la mantisse de ces fractions. Si le dénominateur ne renferme ni le facteur 2 ni le facteur 5, la mantisse sera encore composée de périodes, parceque, pour ce cas, on parviendra aussi à un terme de la suite 10, 100, 1000, etc. qui soit congru à l'unité, suivant le dénominateur, et l'exposant de ce terme, que l'on peut déterminer par le n° 92, indiquera la grandeur de la période, qui est indépendante du numérateur, tant que la fraction est irréductible,



RECHERCHES

Mais si le dénominateur est de la forme  $2^{\alpha} 5^{\beta} N$ ,  $N$  étant un nombre premier avec 10,  $\alpha$  et  $\beta$  des nombres qui ne peuvent être zéro à-la-fois, la mantisse deviendra périodique après les  $\alpha$  ou  $\beta$  premiers chiffres, suivant que  $\alpha$  ou  $\beta$  est le plus grand; ces périodes seront composées d'autant de chiffres que celles des fractions dont le dénominateur est  $N$ . Ceci se déduit facilement de ce que la fraction proposée peut se décomposer en deux autres dont les dénominateurs soient  $2^{\alpha} 5^{\beta}$  et  $N$ , et dont la première sera interrompue après les  $\alpha$  ou  $\beta$  premiers chiffres.

Au reste, nous pourrions ajouter encore beaucoup d'autres observations sur ce sujet, surtout à l'égard des artifices au moyen desquels on peut construire avec une grande facilité la Table III; mais, forcés d'abrégé, nous les omettons d'autant plus volontiers qu'une grande partie a été publiée tant par *Robertson* que par *Bernoulli* (*Nouv. Mém. de l'Acad. de Berlin*, 1771).

TABLE PREMIERE. (n° 58, 91).

3	2	2.	3.	5.	7.11	13.17.19.23.29	31.37.41.43.47
5	2	1.	3				
7	5	2.	1.	5			
9	2	1.	*	5.	4		
11	2	1.	8.	4.	7		
13	6	5.	8.	9.	7.11		
16	5	*	3.	1.	2.	1	5
17	10	10.11.	7.	9.13	12		
19	10	17.	5.	2.12.	6	13.	8
23	10	8.20.15.21.	3	12.17.	5		
25	2	1.	7.	*	5.16	19.13.18.11	
27	2	1.	*	5.16.13	8.15.12.11		
29	10	11.27.18.20.23	2.	7.15.24			
31	17	12.13.20.	4.29	23.	1.22.21.27		
32	5	*	3.	1.	2.	5	7. 4. 7. 6. 3
37	5	11.34.	1.28.	6	15. 5.25.21.15	27	0
41	6	26.15.22.39.	3	51.33.	9.36.	7	28.32
43	28	39.17.	5.	7.	6	40.16.29.20.35	32.35.18
47	10	30.18.17.38.27	3.42.29.39.43	5.24.25.37			
49	10	2.13.41.	*	16	9.31.35.32.24	7.38.27.36.23	
53	20	25.	9.31.38.46	28.42.41.39.	6	45.22.33.30.	8

SUITE DE LA TABLE PREMIERE.

59	10	25.32.34.44.45	23.14.22.27.	4	7.41.	2.13.53
61	10	47.42.14.23.45	20.49.22.39.25	13.33.18.41.40		
64	5	*. 3.	1.10.	5	15.12.	7.14.11
67	12	29. 9.39.	7.61	23.	8.26.20.22	43.44.19.63.64
71	62	58.18.14.33.43	27.	7.58.	5.	4
73	5	59.29.37.11				
79	29	50.71.34.19.70.	74.	9.10.52.	1	76.23.21.47.55
81	11	7.17.75.54.33	4			
83	50	3.52.81.24.72	67.	4.59.16.36	32.60.38.49.69	
89	30	72.87.18.	7.	4	65.82.53.31.29	57.77.67.59.34
97	10	86.	2.11.53.82	83.19.27.79.47	26.41.71.44.60	
		14.65.32.51.25	20.42.91.18			

S U I T E D E L A T A B L E I I I.

67	(0).....0149253731 597	3432855820	89552223880
	(1).....1791044776 164	1194029850	7462686567
71	(0).....0140845070 28169	4225352112	6760563380
	(1).....8722394366 46478	1971850985	9154929577
73	(0).....01369863; (3).....71232876; (6).....04109589;	(1).....06849315; (4).....56164383; (7).....20547945;	(2).....34246575; (5).....80821917; (8).....02739726
79	(0).....0126582278 (2).....645566202 (4).....9240506329	481; 531; 113;	(1).....3670886075 (3).....7215189875 (5).....7974683544
81	(0).....012345679; (2).....493827160; (4).....735086419;	(1).....135802469; (3).....432098765; (5).....283950617	
85	(0).....0120481927 4457851525	7108433734	9597590361
	(1).....6024096385 2891566265	3 5421686746	9879518072
89	(0).....0112359550 4643820224	561797528	0898876404
	(1).....3370786516 8314606741	7191 8539325842	6966292134
97	(0).....0103092783 8762886597 4845360824 185567.	5051546591 9381443298 7422680412	7525775195 969071649 3711340206

T A B L E I I I. (n° 316).

5	(0).....5; (1)....6		
7	(0).....142857		
9	(0).....1; (1)....2; (2)....4; (3)....8; (4)....7; (5)....5		
11	(0).....09; (1)....18; (2)....36; (3)....72; (4)....45		
13	(0).....076923; (1)....461538		
17	(0).....0588235294 117647		
19	(0).....0526315789 47368421		
23	(0).....0434782608 6956521739	13	
27	(0).....037; (1)....074; (2)....148; (3)....296; (4)....592; (5)....185		
29	(0).....054487586	2068965517	24137931
31	(0).....0322258645 16129		
37	(1).....5483870967 74193		
	(0).....027; (1)....135; (2)....675; (3)....378; (4)....891; (4)....459; (6)....297; (7)....486; (8)....432; (9)....162; (10)....810; (11)....054		
41	(0).....02439; (1)....14634; (2)....87804; (3)....26829; (4)....60975; (5)....65853; (6)....95121; (7)....70731		
43	(0).....0232558139 5348837209	3	
	(1).....6511627906 9767441860	4	
47	(0).....0212765957 4468085106	3829787234	
	0425531914 893617		
49	(0).....0204081632 6330612244	8979591836	
	7546938775	51	
53	(0).....0188679245 283; (1)....4905660577	338;	
	(2).....7547169811	320; (3)....6226415094	539
59	(0).....0169491525 4237288135	5952203389	
	8305084745	06779661	
61	(0).....016393426 9856005575	2295081967 7704918052	2151147540 7808852459

## Comportement curieux de la touche $y^x$

Mariza Grand'Henry-Krynska et Pierre Bolly

A travers le problème développé dans cet article nous souhaitons contribuer à la discussion sur l'apprentissage de la démonstration par des élèves du secondaire.

Selon une conception largement répandue, la démonstration serait univoquement définie dans un système hypothético-déductif et surtout elle exclurait tout recours aux données empiriques.

Élaborer une démonstration, ce n'est pas seulement déduire. Dans un problème de recherche, c'est aussi formuler des conjectures et chercher leurs preuves même empiriques.

Plusieurs facettes de cette démarche sont présentes dans les problèmes liés au comportement de la touche  $y^x$ .

### 1. Exploration

Avec la touche  $y^x$  et un nombre  $a$  on peut fabriquer une suite de nombres de la forme

$$a, a^a, a^{(a^a)}, a^{(a^{(a^a)})}, \dots$$

Construisez de telles suites à l'aide de vos calculatrices pour quelques valeurs positives de  $a$ . Que pouvez-vous observer à leur sujet ? Formulez des conjectures <sup>1</sup>.

#### 1.1 Premiers calculs et observations

Pour  $a = 1$ , le résultat est évident.

Formons la première suite pour  $a = 2$ . La calculatrice affiche les trois premiers termes 2, 4, 16 et après, elle signale *overflow*. Cela se comprend aisément : cette suite tend très vite vers l'infini.

Formons la deuxième suite pour  $a = 1,2$ . La calculatrice affiche les termes qui changent jusqu'à la 19ème étape. Par après, le nombre affiché reste le même : 1,257734.

Considérons encore une troisième suite pour  $a = 0,5$ . Les termes affichés ne changent plus à partir du 33ème qui est 0,64118574451.

Dans le cas des deux dernières suites, nous sommes tentés de dire qu'elles convergent vers des nombres dont l'approximation est fournie par la calculatrice quand l'affichage des termes de la suite se stabilise.

Pour des raisons encore obscures ou peut être par analogie avec les suites géométriques de raison plus petite que 1, nous pouvons penser que les suites construites avec un nombre  $a < 1$  sont convergentes. Par contre, la même analogie avec le comportement des suites géométriques de raison plus grande que 1 ne tient pas la route : la suite formée à partir de 2 tend vers l'infini mais celle formée à partir de 1,2 paraît convergente.

<sup>1</sup> Une conjecture est une propriété que l'on a certaines raisons de croire vraie, mais dont on n'est pas entièrement sûr.