Entiers, rationnels et congruences

par Eliane Cousquer
Laboratoire LAMIA [1]

Table des matières

---

1 Les entiers et les rationnels

Le premier document arithmétique de l'histoire, la tablette babylonienne Plimpton 322 établissait une liste de triplets pythagoriciens. Les livres 7 à 9 des Éléments d'EUCLIDE sont un document très riche sur l'étude des propriétés des entiers et des rapports d'entiers. Les livres de DIOPHANTE traitent des problèmes indéterminés à solutions entières et leur redécouverte au dix-septième siècle a eu un rôle très important dans le renouveau de cette science. Que l'on songe à FERMAT

[1] http ://www.lille.iufm.fr/labo/entreelabo2.html

et à son théorème écrit en annotation de l'exemplaire du livre de DIOPHANTE en sa possession, à EULER et à la fonction arithmétique qui porte son nom. Il n'est pas question ici de faire un exposé d'histoire de la théorie des nombres [2], 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 mèlent étroitement informatique, algèbre et arithmétique [3].

1.1 Les Recherches arithmétiques de GAUSS

Au travers d'une telle expérience, nous allons découvrir un aspect du travail de GAUSS, (1777-1855), qui a marqué un tournant dans l'histoire de l'arithmétique. L'idée de départ peut être trouvée dans les *Disquisitiones arithmeticae* (1801) où est exposée la théorie des congruences dans la troisième section, et où sont développées dans la sixième différentes applications dont la théorie des développements décimaux illimités [4]. Avec l'activité présentée ici nous serons fidèles à un aspect des recherches de GAUSS qui a beaucoup expérimenté sur des valeurs particulières, par exemple en confectionnant des tables de valeurs, avant d'induire des résultats qu'il démontrait ensuite (ou pour lesquels il indiquait ne pas avoir encore une démonstration générale). La méthode utilisée ici présente donc aussi un intérêt historique.

L'expérience suppose une lecture active. Une fois le problème en tête, fermez ce livre et essayez, en faisant les calculs proposés, 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.

1.2 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

[2] OYSTEIN ORE, *Number theory and its history* et DICKSON, *History of the theory of numbers*.

[3] Michel DEMAZURE, *Cours d'algèbre, primalité, divisibilité, codes*.

[4] qui figure pages 388 à 398 de la traduction du livre de GAUSS paru aux éditions Blanchard sous le titre *Recherches Arithmétiques*.

dont les seuls diviseurs sont 1 et lui-même. L'entier 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 :

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

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 [5].

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 simplifierons 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 calculettes de collège actuelles disposent aussi d'une fonction de simplification des fractions.

[5] Au moment où l'arithmétique va être réintroduite dans les programmes de terminales, 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.

1.3 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 [6]. 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.

1.4 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.

[6] Par exemple

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

.

1.5 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.
$\frac{1}{3} = 0,33333... = 0,\overline{3} \qquad (0,1) \qquad ; \qquad \frac{2}{3} = 0,66666... = 0,\overline{6} \qquad (0,1)$

Fractions de dénominateur 6 **:** Deux développements comportant un chiffre avant la période et une période d'un seul chiffre.
$\frac{1}{6} = 0,16666... = 0,1\overline{6} \qquad (1,1) \qquad ; \qquad \frac{5}{6} = 0,83333... = 0,8\overline{3} \qquad (1,1)$
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.

$$\frac{1}{7} = 0,142857142857... = 0,\overline{142857} \qquad (0,6)$$
$$\frac{3}{7} = 0,428571428571... = 0,\overline{428571} \qquad (0,6)$$
$$\frac{2}{7} = 0,285714285714... = 0,\overline{285714} \qquad (0,6)$$
$$\frac{6}{7} = 0,857142857142... = 0,\overline{857142} \qquad (0,6)$$
$$\frac{4}{7} = 0,571428571428... = 0,\overline{571428} \qquad (0,6)$$
$$\frac{5}{7} = 0,714285714285... = 0,\overline{714285} \qquad (0,6)$$

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.

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

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

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

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

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

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.

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

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.

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

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

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

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

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

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

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.

$$\frac{1}{14} = 0,0\overline{714285}\,; \quad \frac{3}{14} = 0,2\overline{142857}\,; \quad \frac{9}{14} = 0,6\overline{428571} \qquad (1,6)$$

$$\frac{13}{14} = 0,9\overline{285714}\,; \quad \frac{11}{14} = 0,7\overline{857142}\,; \quad \frac{5}{14} = 0,3\overline{571428} \qquad (1,6)$$

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.

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

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

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.

$$10^7 = 17 \times 588235 + 5 \quad ; \quad \frac{1}{17} = \frac{1}{10^7}(588235 + \frac{5}{17})$$

$$5 \times 10^7 = 17 \times 2941176 + 8 \quad ; \quad \frac{5 \times 10^7}{17 \times 10^{14}} = \frac{1}{10^{14}}(2941176 + \frac{8}{17})$$

$$8 \times 10^2 = 17 \times 47 + 1 \quad ; \quad \frac{8 \times 10^2}{17 \times 10^{16}} = \frac{1}{10^{16}}(47 + \frac{1}{17})$$

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

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.

$$6 = 2 \times 3 \quad (n = 1) \qquad ; \qquad 12 = 4 \times 3 \quad (n = 2)$$
$$14 = 2 \times 7 \quad (n = 1) \qquad ; \qquad 15 = 5 \times 3 \quad (n = 1)$$

Fractions de dénominateur 6 **:**

$\frac{1}{6} = 0,16666... = \frac{5}{10\times3} = \frac{1}{10}(1 + \frac{2}{3})$; $\frac{5}{6} = 0,83333... = \frac{25}{10\times3} = \frac{1}{10}(8 + \frac{1}{3})$

Fractions de dénominateur 12 **:**

$\frac{1}{12} = 0,08\overline{3} = \frac{25}{100\times3} = \frac{1}{100}(8 + \frac{1}{3})$; $\frac{5}{12} = 0,41\overline{6} = \frac{125}{100\times3} = \frac{1}{100}(41 + \frac{2}{3})$

$\frac{7}{12} = 0,58\overline{3} = \frac{175}{100\times3} = \frac{1}{100}(58+\frac{1}{3})$; $\frac{11}{12} = 0,91\overline{6} = \frac{275}{100\times3} = \frac{1}{100}(91+\frac{2}{3})$

Fractions de dénominateur 14 **:**

$\frac{1}{14} = 0,0\overline{714285} = \frac{5}{10\times7} = \frac{1}{10}(0 + \frac{5}{7})$; $\frac{3}{14} = 0,2\overline{142857} = \frac{15}{10\times7} = \frac{1}{10}(2 + \frac{1}{7})$

$\frac{5}{14} = 0,3\overline{571428} = \frac{25}{10\times7} = \frac{1}{10}(3 + \frac{4}{7})$; $\frac{9}{14} = 0,6\overline{428857} = \frac{45}{10\times7} = \frac{1}{10}(6 + \frac{3}{7})$

$\frac{11}{14} = 0,7\overline{857142} = \frac{55}{10\times7} = \frac{1}{10}(7 + \frac{6}{7})$; $\frac{13}{14} = 0,9\overline{285714} = \frac{65}{10\times7} = \frac{1}{10}(9 + \frac{2}{7})$

Fractions de dénominateur 15 **:**

$\frac{1}{15} = 0,0\overline{6} = \frac{2}{10\times3} = \frac{1}{10}(0 + \frac{2}{3})$; $\frac{2}{15} = 0,1\overline{3} = \frac{4}{10\times3} = \frac{1}{10}(1 + \frac{1}{3})$

$\frac{4}{15} = 0,2\overline{6} = \frac{8}{10\times3} = \frac{1}{10}(2 + \frac{2}{3})$; $\frac{7}{15} = 0,4\overline{6} = \frac{14}{10\times3} = \frac{1}{10}(4 + \frac{2}{3})$

$\frac{8}{15} = 0,5\overline{3} = \frac{16}{10\times3} = \frac{1}{10}(5 + \frac{1}{3})$; $\frac{11}{15} = 0,7\overline{3} = \frac{22}{10\times3} = \frac{1}{10}(7 + \frac{1}{3})$

$\frac{13}{15} = 0,8\overline{6} = \frac{26}{10\times3} = \frac{1}{10}(8 + \frac{2}{3})$; $\frac{14}{15} = 0,9\overline{3} = \frac{28}{10\times3} = \frac{1}{10}(9 + \frac{1}{3})$

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

$a = b$ $\quad \frac{p}{q} = \frac{1}{10^a} \times \frac{p}{q'}$ $\quad p = mq' + r$ et $\frac{p}{q} = \frac{1}{10^a} \times (m + \frac{r}{q'})$

$a < b$ $\quad \frac{p}{q} = \frac{1}{10^b} \times \frac{p\times2^{b-a}}{q}$ $\quad p\times2^{b-a} = mq' + r$ et $\frac{p}{q} = \frac{1}{10^b} \times (m + \frac{r}{q'})$

$a > b$ $\quad \frac{p}{q} = \frac{1}{10^a} \times \frac{p\times5^{a-b}}{q}$ $\quad p\times5^{a-b} = mq' + r$ et $\frac{p}{q} = \frac{1}{10^a} \times (m + \frac{r}{q'})$

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 $\frac{1}{7}$.

$$\begin{array}{cccccc|l} 1 & 0 & & & & & 7 \\ & 3 & 0 & & & & \overline{0,142857} \\ & & 2 & 0 & & & \\ & & & 6 & 0 & & \\ & & & & 4 & 0 & \\ & & & & & 5 & 0 \\ & & & & & & 1 \end{array}$$

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 avions 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 [7].

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 :
$10^{n+i} \equiv 10^n \quad \text{mod } q$
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.

[7] c'est-à-dire en prenant le reste dans la division par 13 du nombre obtenu.

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. Cherchons les développements et les familles 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.

$1/21$									$2/21$							
	Q	0,	0	4	7	6	1	9		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
		5	6	5	2	1	7	3	9	1	3			
	R	1	10	8	11	18	19	6	14	2	20	16	22	13
		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
	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
	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-on modulo q ?*

2 Les congruences

Nous allons illustrer la théorie des congruences, les résidus de puissances et en particulier la notion de racine primitive [8]. Nous allons introduire par des exemples les théorèmes établis par GAUSS [9]. 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.

[8] Là encore, nous pourrions expérimenter pour induire des résultats avant de voir le contenu du livre de GAUSS. Cela donnerait de nombreuses activités.

[9] Chaque énoncé sera suivi de sa référence dans le texte de GAUSS.

2.1 La théorie des congruences

La notion de congruence [10] est définie dans le premier chapitre, ainsi que les propriétés élémentaires des résidus modulo n. La suite 1, 2, ..., $n-1$ 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 :

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

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

Le second chapitre est consacré aux congruences du premier degré. Il commence par le théorème dit de GAUSS [11], l'unique décomposition des entiers en facteurs premiers [12] et ses applications élémentaires [13]. GAUSS traite ensuite la résolution des congruences du premier degré $ax + by = c$ et les problèmes apparentés [14].

2.2 Nombre de fractions irréductibles de dénominateur p

Cela revient au problème suivant [15] 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

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

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

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

[10] $a \equiv b$ modulo $n \Longleftrightarrow a - b$ divisible par n

[11] paragraphe 14.
[12] paragraphe 16.
[13] paragraphes 17 à 23.
[14] paragraphes 24 à 37.
[15] paragraphe 38

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

$$A = a^{\alpha}b^{\beta}c^{\gamma} \Longrightarrow \phi(A) = A(1-\frac{1}{a})(1-\frac{1}{b})(1-\frac{1}{c})...$$

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 $18/6$.

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

Si nous écrivons les 18 fractions de dénominateurs 18, après simplification, elles se répartissent en fractions ayant pour dénominateurs les différents 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 [16] on obtient [17] :

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

Nous avons introduit là la *fonction d'Euler* dont GAUSS cite deux articles en référence [18]. GAUSS démontre [19] le résultat que nous avons illustré avec notre tableau :

> Si a, a', a'' sont tous les diviseurs de A [20], on aura :
>
> $$A = \phi(a) + \phi(a') + \phi(a'') + ...$$

2.3 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 [21] :

> Dans toute progression géométrique 1, a, a^2, a^3... 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, ...,a^t... 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 $a^{mt} \equiv 1 \mod p$

$$a^r \equiv a^\rho \iff r \equiv \rho \bmod t$$

Les t restes qui composent la période sont tous différents.

---

[16] Cette méthode n'est pas dans le livre de GAUSS, mais elle nous paraît très éclairante.

[17] en posant $\phi(1) = 1$.

[18] *Theoremata arithmetica nova methodo demonstrata* comment. nov. acc.Petrop. VIII page 74 et *Speculationes circa quasdam insignes proprietates numerorum* Acta Patrop. VIII p 17.

[19] paragraphe 39.

[20] 1 y compris.

[21] paragraphe 45.

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 9×9 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.

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 [22] de $p-1$ [23].

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

[22] un diviseur de $p-1$.

[23] Théorème 49. On dirait «l'ordre de a est $p-1$ ou un diviseur de $p-1$».

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... a^t divise $p-1$.

C'est là le théorème [24] dont FERMAT assurait avoir trouvé une démonstration qu'il n'a pas publiée, et dont EULER a fourni deux démonstrations présentées brièvement par GAUSS [25] avec leurs références [26].

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.

2.4 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 [27] 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 [28], qui n'est pas vrai pour certains entiers. GAUSS va s'intéresser de façon approfondie aux racines primitives modulo un nombre premier [29].

[24] appelé petit théorème de Fermat.

[25] paragraphe 50.

[26] *Fermatii opera math. Tolosae* 1679 Fol. p 163 et *Démonstration de quelques théorèmes 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.

[27] paragraphes 54 et 55.

[28] paragraphe 56.

[29] paragraphes 49 à 81.

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 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 est 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'ordre 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 [30] :

[30] paragraphe 58.

> 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.
>
> 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 [31]

> 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 [32]. 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 [33].

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 :

[31] paragraphe 73.
[32] paragraphe 72.
[33] à partir du paragraphe 82.

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 [34] premier avec m, qui est congrue à l'unité suivant le module m sera égal à f ou une partie aliquote [35] de f.

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 [36]. 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 [37] 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 $p = 15$.

[34] l'ordre de a.

[35] paragraphe 83. C'est le *théorème d'Euler* (1760) ; curieusement GAUSS cite ce résultat sans faire référence à EULER.

[36] 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.

[37] paragraphe 88 et 89.

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

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 [38] 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 $2 \times p^n$.

[38] paragraphe 90.

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 [39]**.**

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 [40] 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.

2.5 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 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 [41].

3 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.

3.1 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

[39] paragraphe 92.

[40] *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).

[41] DICKSON, *History of the theory of numbers*.

fractions irréductibles de dénominateurs a et b [42].

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

Il en déduit que toute fraction peut s'écrire, si son dénominateur a pour décomposition en facteurs premiers $n = a^\alpha \times b^\beta \times c^\gamma ...$ de façon unique sous la forme d'une somme d'un entier et de fractions [43] plus petites que 1 :

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

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.

3.2 Fractions de dénominateurs p^n

Nous avons vu que le développement des fractions $\frac{10 \times m}{p^n}$, $\frac{10^2 \times m}{p^n}$... $\frac{10^e \times m}{p^n}$ 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 :

$$(0).....0588235294117647$$

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 $16 \equiv 10^8$

[42] paragraphe 309
[43] paragraphe 310

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 $5 + 9 = 14 \equiv 2$ 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.

$$(0) \quad ...076923 \quad ; \quad (1) \quad ...461538$$

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 $11 \equiv 6^{2\times5} \times 6^1$ 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 $12 \equiv 6^{2\times3}$, $12 \equiv 6^{2\times3}$ 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	×	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 :

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

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^μ, si $10^e \equiv 1$ modulo p^μ, 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 [44] et GAUSS fait figurer dans sa table de développements, les développements des fractions $\frac{1}{p^\mu}$, $\frac{a}{p^\mu}$, $\frac{a^2}{p^\mu}$, $\frac{a^3}{p^\mu}$...$\frac{a^{f-1}}{p^\mu}$.

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 [45].

[44] paragraphe 71.

[45] paragraphe 315

3.3 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.

4 Bibliographie

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