ETUDE SUR LES NOMBRES TETUS ET LES NOMBRES PREMIERS LONGS

Rodolphe LAMPE

Juillet 2005

Epreuve de projet - ENS Lyon

Table des matières

I	Periodicité dans $\mathbb{Q} \setminus \mathbb{D}$	3
1	Développement décimal infini	3
2	Périodicité	3
3	Période et motif dans l'écriture fractionnaire	4
4	Inverse d'un nombre premier	4
II	Racines primitives et nombres premiers longs	5
5	Racine primitive	5
5.1	Définitions et propriétés	5
5.2	Lien avec la fonction indicatrice d'Euler	5
6	Les nombres premiers longs	6
6.1	Définition	6
6.2	Répartition	6
6.3	Périodicité de l'inverse d'un nombre premier long	7
III	Définition et propriétés des nombres têtus	8
7	Définition	8
8	Propriété des multiples	8
9	Propriété des multiples n^2	9
10	Théorème de Midy	10
11	Extension du théorème de Midy	11
IV	La conjecture d'Artin	12
12	Enoncé de la conjecture	12
13	Un début de preuve de l'infinité des nombres premiers longs	12
14	Probabilités	13

Cet exposé a pour but d'étudier des nombres très particuliers : les nombres dit "têtus". Ceux-ci sont implicitement liés au petit théorème de Fermat. La première partie de cet exposé est une introduction qui permet d'établir quelques résultats assez faciles sur le développement décimal de certains rationnels. On introduit ici les notions de motif et période. La seconde partie permet d'introduire les bases mêmes des nombres têtus : les racines primitives et les nombres premiers longs. La troisième partie est la plus importante de toutes, à l'aide des deux premières parties on peut ici définir les nombres têtus et en montrer leurs propriétés fondamentales. La quatrième partie donne et explique la formule donnant la densité des nombres premiers longs parmi les nombres premiers.

Première partie

Periodicité dans $\mathbb{Q} \setminus \mathbb{D}$

1 Développement décimal infini

Théorème

Tout nombre rationnel non décimal possède un développement décimal infini.

Preuve :

Soit $x \in \mathbb{Q} \setminus \mathbb{D}$. Par l'absurde, supposons que x possède un développement décimal fini¹ alors il existe n entier a_i compris entre 0 et 9 tel que

$$x = a_1 a_2 \dots a_k, a_{k+1} \dots a_n$$

On pose $a = a_1 a_2 \dots a_n$ alors

$$x = \frac{a}{10^{n-k}}$$

$x \in \mathbb{D}$, absurde.

2 Périodicité

Théorème

Tout nombre rationnel non décimal a son développement décimal périodique à partir d'un certain rang.

Preuve :

Soit $x = \frac{a}{b}$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, $a \wedge b = 1$ et b possède un diviseur premier différent de 2 et 5 (sinon $x \in \mathbb{D}$).

Effectuons la division euclidienne de a par b :

$$\begin{aligned} a &= q_1 \times b + r_1 \\ 10 \times r_1 &= q_2 \times b + r_2 \\ 10 \times r_2 &= q_3 \times b + r_3 \\ &\dots \\ 10 \times r_{n-1} &= q_n \times b + r_n \\ &\dots \end{aligned}$$

¹On peut définir le terme "développement décimal fini" de deux façons :

- à partir d'un certain rang le développement décimal est une suite infinie de zéros.

- le nombre x possède un développement décimal fini si il possède deux développements décimal différent (par exemple $1,000\dots = 0,999\dots$).

Les q_i donnent le développement décimal de x (On prend a strictement inférieur à $10 \times b$ pour que q_1 soit bien inférieur ou égal à 9, le cas a supérieur à $10 \times b$ se résout de la même façon en étudiant $y = x - E(x)$).

Tout les r_i sont des entiers compris entre 0 et $b - 1$ donc il existe j et $k \leq b - 1$ fixés tel que $r_j = r_{j+k}$ (on ne peut pas avoir une suite d'entiers bornés et tous différents, c'est le principe des tiroirs).

Montrons que pour tout $i \geq j$, $r_i = r_{i+k}$ en effet par récurrence :

$$r_n = r_{n+k} \Rightarrow 10 \times r_n \equiv 10 \times r_{n+k}(b) \Rightarrow r_{n+1} \equiv r_{n+1+k}(b) \Rightarrow r_{n+1} = r_{n+1+k}$$

La suite (r_n) étant périodique de période k , la suite (q_n) est elle aussi k -périodique par construction. Le développement décimal de x est donc périodique de période k et de motif $q_j q_{j+1} \dots q_{j+k-1}$.

3 Période et motif dans l'écriture fractionnaire

Soit $x \in \mathbb{Q} \setminus \mathbb{D}$, on a vu précédemment que x était périodique à partir d'un certain rang, faisons apparaître le motif m (le groupe de chiffres se répétant dans le développement décimal) et la période p (nombre de chiffres du motif) dans l'écriture fractionnaire de x .

Si le développement décimal de x est périodique au bout de i chiffres, on définit y tel que $y = 10^i \times x - E(10^i \times x)$ ainsi y a une partie entière nulle et le développement décimal est périodique juste après la virgule.

On définit $m = m_1 \dots m_p$ le motif avec (m_i) les chiffres du motif et p la période.

$$y = 0, m_1 \dots m_p m_1 \dots m_p \dots$$

$$10^p \times y - y = m_1 \dots m_p, m_1 \dots m_p \dots - 0, m_1 \dots m_p \dots = m_1 \dots m_p = m$$

$$y = \frac{m}{10^p - 1}$$

On pouvait aussi démontrer cette formule en remarquant que y était la somme des termes d'une suite géométrique de raison 10^{-p} et de premiers terme $m \cdot 10^{-p}$.

On obtient alors $10^i \times x = E(10^i \times x) + y$ donc

$$x = \frac{E(10^i \times x)}{10^i} + \frac{m}{10^i(10^p - 1)}$$

4 Inverse d'un nombre premier

Théorème

La période de l'inverse d'un nombre premier p différent de 2 et 5 divise $p - 1$.

Preuve :

Soit p un nombre premier différent de 2 et 5 alors $\frac{1}{p}$ est un nombre rationnel non décimal. On note $\dot{x}$ la classe de x dans $\mathbb{Z}/p\mathbb{Z}$.

Soit $G = \{10^x, x \in \mathbb{N}\}$, on vérifie facilement que G muni de la loi multiplicative est un sous-groupe cyclique de $(\mathbb{Z}/p\mathbb{Z})^*$, $(\times)$ (10 est inversible car p est différent de 2 et 5). Soit q son cardinal alors q est le plus petit entier vérifiant $10^q \equiv 1(p)$ et d'après le théorème de Lagrange $q \mid p - 1$.

On définit m par $m = \frac{10^q - 1}{p}$ et finalement on obtient bien

$$\frac{1}{p} = \frac{m}{10^q - 1}, q \mid p - 1$$

Une seconde méthode pour démontrer que $q \mid p - 1$ est de montrer que le reste r de la division euclidienne de $p - 1$ par q est inférieur à q et vérifie $10^r \equiv 1(p)$ donc $r = 0$ par minimalité de q .

Deuxième partie

Racines primitives et nombres premiers longs

5 Racine primitive

Par abus de langage, on notera pour un entier a : $a \in \mathbb{Z}/p\mathbb{Z}$ au lieu de $\text{classe}(a) \in \mathbb{Z}/p\mathbb{Z}$.

5.1 Définitions et propriétés

Définition de l'ordre d'un élément

L'ordre d'un élément a de $\mathbb{Z}/p\mathbb{Z}$ non nul est la plus petite puissance non nulle k tel que $a^k \equiv 1(p)$, l'ordre existe pour tout élément non nul car le théorème de Fermat donne $a^{p-1} \equiv 1(p)$

Définition d'une racine primitive

a est une racine primitive du nombre premier p différent de 2 et 5 si l'ordre de a est égale à $p-1$

Théorème

a est une racine primitive du nombre premier p différent de 2 et 5 si et seulement si pour tout $n \in (\mathbb{Z}/p\mathbb{Z})^*$ il existe $x_n \in \mathbb{Z}/(p-1)\mathbb{Z}$ tel que $n \equiv a^{x_n}(p)$

Preuve :

Soit f le morphisme de groupe de $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ dans $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ défini² par $f(k) \equiv a^k(p)$. En effet on a bien :

$$f(x+y) \equiv a^{x+y} \equiv a^x \times a^y \equiv f(x) \times f(y)(p)$$

$\mathbb{Z}/(p-1)\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z})^*$ ont même cardinal, il suffit donc de montrer que f est injectif ou surjectif pour montrer que f est un isomorphisme.

Par l'absurde supposons qu'il existe $x, y \in \mathbb{Z}/(p-1)\mathbb{Z}$ tel que $f(x) = f(y)$ et $x \neq y$ par exemple $x > y$.

$$f(x) = f(y) \Leftrightarrow a^x \equiv a^y(p) \Leftrightarrow a^{x-y} \equiv 1(p)$$

$0 < x-y < p-1$ donc a n'est pas une racine primitive de p , absurde.

f est injectif c'est donc un isomorphisme. f possède donc un isomorphisme réciproque qui à tout n de $(\mathbb{Z}/p\mathbb{Z})^*$ associe un unique x_n (car f^{-1} est un isomorphisme) de $\mathbb{Z}/(p-1)\mathbb{Z}$ tel que $n \equiv a^{x_n}(p)$.

Théorème

Si a est une racine primitive du nombre premier p différent de 2 et 5 alors $\mathbb{Z}/p\mathbb{Z} = \langle a \rangle$

Preuve : On considère le morphisme f précédent. On a vu que a est une racine primitive implique que f est un isomorphisme donc $\forall n \in \mathbb{Z}/p\mathbb{Z}, \exists x_n \in \mathbb{N}$ tel que $a^{x_n} \equiv n(p)$ donc $\langle a \rangle = \mathbb{Z}/p\mathbb{Z}$

5.2 Lien avec la fonction indicatrice d'Euler

Théorème

Tout nombre premier p possède $\varphi(p-1)$ racines primitives, φ étant la fonction indicatrice d'euler donnant le nombre d'entiers inférieurs et premiers à $p-1$.

²On définit la fonction puissance pour $x \in \mathbb{N}$ et $\text{classe}(x) \in \mathbb{Z}/(p-1)\mathbb{Z}$ ainsi : $a^{\text{classe}(x)} \equiv a^x(p)$

Preuve : Soit a une racine primitive modulo p (dont on suppose l'existence). Si n est premier avec $p - 1$ alors a^n est une racine primitive car si l'ordre de a^n est égale à $q < p - 1$ alors a^{nq} est égale à 1 or nq est différent de $p - 1$ (car $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un anneau intègre) donc a n'est pas racine primitive : absurde. Donc pour tout n premier avec $p - 1$, a^n est une racine primitive. Comme $\langle a \rangle = \mathbb{Z}/p\mathbb{Z}$, il y a au moins $\varphi(p - 1)$ racines primitives, il suffit maintenant de montrer que si n n'est pas premier avec $p - 1$ alors a^n n'est pas une racine primitive. Soit $d \neq 1$ tel que d divise n et $p - 1$ alors l'ordre de a^n est $\frac{p-1}{d}$ car $a^{n \times \frac{p-1}{d}} \equiv a^{(p-1) \times \frac{n}{d}} \equiv 1(p)$.
Donc il y a $\varphi(p - 1)$ racines primitives modulo p .

6 Les nombres premiers longs

6.1 Définition

Définition d'un nombre premier long

Un nombre premier p est un nombre premier long si et seulement si 10 est une racine primitive modulo p .

6.2 Répartition

Les nombres premiers longs inférieurs à 1000 sont :

7, 17, 19, 23, 29, 47, 59, 61, 97, 109,
113, 131, 149, 167, 179, 181, 193, 223, 229, 233,
257, 263, 269, 313, 337, 367, 379, 383, 389, 419,
433, 461, 487, 491, 499, 503, 509, 541, 571, 577,
593, 619, 647, 659, 701, 709, 727, 743, 811, 821,
823, 857, 863, 887, 937, 941, 953, 971, 977, 983.

Il y a 60 nombres premiers longs inférieurs à 1000 et 168 nombres premiers inférieurs à 1000 soit une répartition sur $[0; 1000]$ de $\frac{60}{168} = 0,35714\dots$

Si l'on calcul la densité des nombres premiers longs inférieurs à n parmi les nombres premiers inférieurs à n on remarque que lorsque n tend vers l'infini la densité tend vers une constante égale à 0,37395581..., c'est la constante d'Artin défini par :

$$C_{artin} = \prod_{p \in \mathcal{P}} 1 - \frac{1}{p(p-1)}$$

Cette surprenante formule sera étudié dans la quatrième partie.

6.3 Périodicité de l'inverse d'un nombre premier long

Théorème

Soit p un nombre premier long alors le développement décimal de $\frac{1}{p}$ est périodique de période $p - 1$.

Preuve : p est un nombre premier long donc 10 est une racine primitive modulo p . On a vu dans la première partie que la période de l'inverse d'un nombre premier p est un diviseur de $p - 1$, montrons que la période de $\frac{1}{p}$ est $p - 1$ quand p est premier long.

Par l'absurde, supposons que la période soit égale à $k < p - 1$ alors :

$$\frac{1}{p} = 0, m_1 \dots m_k m_1 \dots m_k \dots \Rightarrow \frac{10^k - 1}{p} = m_1 \dots m_k$$

Donc $10^k \equiv 1(p)$ absurde car 10 est une racine primitive, donc la période de $\frac{1}{p}$ est $p - 1$. Son motif est très particulier, on l'appelle "nombre têtu".

Troisième partie

Définition et propriétés des nombres têtus

Ces nombres sont nommés têtus car ils semblent apprécier la suite de chiffres qui les composent (propriété des multiples, propriété des multiples n°2) et les suites de chiffres 9 (théorème de Midy et son extension).

7 Définition

Définition d'un nombre têtu

Un nombre têtu est lié à un nombre premier long p par la formule :

$$m = \frac{10^{p-1} - 1}{p}$$

m est le motif du développement décimal de la fraction $\frac{1}{p}$

Clairement m est bien un entier par le théorème de Fermat.

Les 5 premiers nombres têtus sont³ :

142857

0588235294117647

052631578947368421

0434782608695652173913

0344827586206896551724137931

8 Propriété des multiples

Propriété des multiples

Soit m le nombre têtu lié au nombre premier long p alors les nombres $m \times 1, m \times 2, \dots, m \times (p - 1)$ possèdent les mêmes chiffres rangés dans le même ordre.

Exemple :

$$\begin{aligned} 142857 \times 1 &= 142857 \\ 142857 \times 2 &= 285714 \\ 142857 \times 3 &= 428571 \\ 142857 \times 4 &= 571428 \\ 142857 \times 5 &= 714285 \\ 142857 \times 6 &= 857142 \end{aligned}$$

C'est la première propriété remarquable des nombres têtus.

En voici la preuve :

Soit $m = m_1 \dots m_{p-1}$ où $\frac{1}{p} = 0, m_1 \dots m_{p-1} m_1 \dots$ alors pour k fixé dans $\{1; \dots; p - 1\}$:

³On "garde" les zéros au début des nombres têtus car ceux-ci sont aussi des motifs et le zéro est alors nécessaire pour définir la position du chiffre qu'il précède

$$\begin{aligned} m_{k+1} \dots m_1 m_{p-1} \dots m_k &= (10^{p-1} - 1) \times 0, m_{k+1} \dots m_1 m_{p-1} \dots m_k m_{k+1} \dots m_1 m_{p-1} \dots m_k \dots \\ &= (10^{p-1} - 1) \times (10^k \times \frac{1}{p} - m_1 \dots m_k) \end{aligned}$$

On a donc

$$10^k \times \frac{1}{p} - m_1 \dots m_k = \frac{m_{k+1} \dots m_1 m_{p-1} \dots m_k}{10^{p-1} - 1}$$

donc $10^k \times \frac{1}{p} - m_1 \dots m_k$ est compris entre 0 et 1, si on effectue la division euclidienne de 10^k par p on obtient : $10^k = q_k \times p + r_k$ donc $(q_k \times p + r_k) \times \frac{1}{p} - m_1 \dots m_k = q_k - m_1 \dots m_k + \frac{r_k}{p}$ donc $q_k - m_1 \dots m_k = 0$ et finalement on a

$$m_{k+1} \dots m_1 m_{p-1} \dots m_k = r_k \times \frac{10^{p-1} - 1}{p} = r_k \times m_1 \dots m_{p-1}$$

Or $10^k \equiv r_k (p)$ et on a vu précédemment que $\langle 10 \rangle = \mathbb{Z}/p\mathbb{Z}$ donc si on définit $f : k \mapsto r_k$ alors f va de $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ dans $(\mathbb{Z}/p\mathbb{Z}, \times)^*$ et f est un isomorphisme (nous l'avons prouvé précédemment en 5.1) donc pour tout r dans $\{1; \dots; p-1\}$ on a :

$$r \times m_1 \dots m_{p-1} = m_{f^{-1}(r)+1} \dots m_1 m_{p-1} \dots m_{f^{-1}(r)}$$

9 Propriété des multiples n°2

Propriété des multiples n°2

Soit $m = m_1 \dots m_{p-1}$ un nombre têté et k un entier inférieur à $\frac{10^{2(p-1)}}{m}$, si l'on effectue la division euclidienne de $m \times k$ par 10^{p-1} : $m \times k = n_1 \times 10^{p-1} + n_2$ alors m divise $n_1 + n_2$.

Exemple sur 142857 et $k = 142857$ puis 888 :

$$\begin{array}{rclclcl} 142857^2 & = & 20408122449 & & 20408 + 122449 & = & 142857 \\ 142857 \times 888 & = & 126857016 & & 126 + 857016 & = & 857142 \end{array}$$

Ma preuve n'est pas complète car je suppose que $n_1 + n_2 < 10^{p-1}$, en fait si $n_1 + n_2 \geq 10^{p-1}$ il faut réitérer l'algorithme (division euclidienne par 10^{p-1} pour obtenir n'_1 et n'_2 et ainsi de suite jusqu'à obtenir $n'_1 + n'_2 < 10^{p-1}$).

Soit donc $x = m \times k = x_1 \dots x_{2(p-1)}$ (on prend en compte les zéros, c'est à dire que $x_1, x_2, \dots$ peuvent être des zéros en effet la position est ici aussi importante que le chiffre et l'on doit garder une taille "fixe" pour le motif, on a bien $2(p-1)$ chiffres car $k < \frac{10^{2(p-1)}}{m}$). On doit donc montrer que $x_1 \dots x_{p-1} + x_p \dots x_{2(p-1)}$ est un multiple de m . On a :

$$\frac{x}{10^{2(p-1)} - 1} = 0, x_1 \dots x_{2(p-1)} x_1 \dots \quad \text{et} \quad 10^{p-1} \times \frac{x}{10^{2(p-1)} - 1} = x_1 \dots x_{p-1}, x_p \dots x_{2(p-1)} x_1 \dots$$

Si l'on suppose que $n_1 + n_2 < 10^{p-1}$ alors on peut écrire $n_1 + n_2 = x_1 \dots x_{p-1} + x_p \dots x_{2(p-1)} = y_1 \dots y_{p-1}$ et donc

$$(10^{p-1} + 1) \times \frac{x}{10^{2(p-1)} - 1} = x_1 \dots x_{p-1}, y_1 \dots y_{p-1} y_1 \dots$$

Or

$$(10^{p-1} + 1) \times \frac{x}{10^{2(p-1)} - 1} = \frac{x}{10^{p-1} - 1} = \frac{m \times k}{10^{p-1} - 1} = k \times \frac{1}{p}$$

$y_1 \dots y_{p-1}$ est le motif d'un multiple de $\frac{1}{p}$ c'est donc un multiple du motif de $\frac{1}{p}$ d'après la propriété des multiples, donc $n_1 + n_2$ est un multiple de m . On a :

$$n_1 = \left[\frac{k}{p} \right] \quad n_2 = m \times k - 10^{p-1} \times \left[\frac{k}{p} \right]$$

Pour k supérieur à $\frac{10^{2(p-1)}}{m}$, il faut "séparer" $m \times k$ en $l = \left\lceil \frac{[\log(m \times k)]}{p-1} \right\rceil + 1$ puis calculer la somme des l "morceaux".

Exemple avec 142857 et 8574596 :

$$142857 \times 8574596 = 1224941060772 \quad 1 + 224941 + 060772 = 285714$$

10 Théorème de Midy

Théorème de Midy

Soit nombre têtue m composé de $p-1$ chiffres, si l'on "sépare" m en deux⁴ : $m' = m_1 \dots m_{\frac{p-1}{2}}$ et $m'' = m_{\frac{p-1}{2}+1} \dots m_{p-1}$ alors $m' + m'' = 10^{\frac{p-1}{2}} - 1$.

Plus simplement, si l'on sépare un nombre têtue en deux morceaux puis qu'on en fait la somme on obtient $\frac{p-1}{2}$ fois le chiffre 9.

Par exemple : $142 + 857 = 999$ ou $05882352 + 94117647 = 99999999$.

Preuve :

$$\frac{10^{\frac{p-1}{2}} + 1}{p} = m_1 \dots m_{\frac{p-1}{2}}, m_{\frac{p-1}{2}+1} \dots + 0, m_1 \dots m_{p-1} m_1 \dots$$

Or p divise $10^{\frac{p-1}{2}} + 1$ car $10^{p-1} - 1 = (10^{\frac{p-1}{2}} + 1)(10^{\frac{p-1}{2}} - 1)$ et p ne peut diviser $10^{\frac{p-1}{2}} - 1$ car 10 est racine primitive donc d'après le théorème de Gauss p divise $10^{\frac{p-1}{2}} + 1$ donc $\frac{10^{\frac{p-1}{2}} + 1}{p}$ est entier et

$$\frac{10^{\frac{p-1}{2}} + 1}{p} = m_1 \dots m_{\frac{p-1}{2}} + 1$$

$$m' = \frac{10^{\frac{p-1}{2}} + 1 - p}{p}$$

Donc

$$\begin{aligned} m'' &= m_1 \dots m_{p-1} - 10^{\frac{p-1}{2}} \times m_1 \dots m_{\frac{p-1}{2}} \\ &= \frac{10^{p-1} - 1}{p} - 10^{\frac{p-1}{2}} \times \frac{10^{\frac{p-1}{2}} + 1 - p}{p} \\ &= \frac{(p-1)10^{\frac{p-1}{2}} - 1}{p} \end{aligned}$$

Finalement

$$m' + m'' = \frac{(10^{\frac{p-1}{2}} + 1 - p) + ((p-1)10^{\frac{p-1}{2}} - 1)}{p} = 10^{\frac{p-1}{2}} - 1$$

⁴ $\frac{p-1}{2}$ est bien entier puisque p est impair car 2 n'est pas un nombre premier long

11 Extension du théorème de Midy

Soit d un diviseur de $p - 1$ alors si l'on "sépare" m en $\frac{p-1}{d}$ "morceaux" la somme de celles-ci est divisible par $10^d - 1$. Soit plus rigoureusement :

$$m = m_1 \dots m_{p-1}, \forall d, d|p-1 \Rightarrow 10^d - 1 \mid \sum_{i=0}^{\frac{p-1}{d}-1} m_{id+1} \dots m_{id+d}$$

Je n'ai trouvé aucune preuve de cette "extension" ni aucun texte ne parlant de celui-ci, j'espère donc que ma preuve est correcte. Voici tout d'abord quelques exemples qui permettent de mieux visualiser l'énoncé :

$$\begin{array}{llll} m = 142857 & d = 2 & 14 + 28 + 57 & = 1 \times 99 \\ m = 0588235294117647 & d = 4 & 0588 + 2352 + 9411 + 7647 & = 2 \times 9999 \\ m = 0588235294117647 & d = 2 & 05 + 88 + 23 + 52 + 94 + 11 + 76 + 47 & = 4 \times 99 \\ m = 052631578947368421 & d = 6 & 052631 + 578947 + 368421 & = 1 \times 999999 \\ m = 052631578947368421 & d = 3 & 052 + 631 + 578 + 947 + 368 + 421 & = 3 \times 999 \end{array}$$

Preuve :

Soit d un diviseur de $p - 1$. 10 est une racine primitive modulo p et p divise

$$10^{p-1} - 1 = (10^d - 1) \times \sum_{i=0}^{\frac{p-1}{d}-1} 10^{id}$$

donc d'après le théorème de Gauss p divise $\sum_{i=0}^{\frac{p-1}{d}-1} 10^{id}$ car p ne peut diviser $10^d - 1$ (sinon 10 ne serait pas racine primitive). Donc

$$\frac{\sum_{i=0}^{\frac{p-1}{d}-1} 10^{id}}{p} = 0, m_1 \dots + m_1 \dots m_d, m_{d+1} \dots + \dots + m_1 \dots m_{p-1-d}, m_{p-d} \dots \text{ est entier}$$

Donc $0, m_1 \dots + 0, m_{d+1} \dots + \dots + 0, m_{p-d} \dots$ est entier (par exemple n), or

$$(10^{p-1} - 1)(0, m_1 \dots + 0, m_{d+1} \dots + \dots + 0, m_{p-d} \dots) = m_1 \dots m_{p-1} + m_{d+1} \dots m_d + \dots + m_{p-d} \dots m_{p-1-d}$$

et si on note $M_i = m_{1+id} \dots m_{(i+1)d}$ alors

$$m_1 \dots m_{p-1} + m_{d+1} \dots m_d + \dots + m_{p-d} \dots m_{p-1-d}$$

est égal à

$$(M_1 \times 10^{p-1-d} + M_2 \times 10^{p-1-2d} + \dots + M_{\frac{p-1}{d}-1} \times 10^0) + \dots + (M_{\frac{p-1}{d}-1} \times 10^{p-1-d} + \dots + M_{\frac{p-1}{d}-2} \times 10^0)$$

égal à

$$M_1(10^0 + 10^d + \dots + 10^{p-1-d}) + \dots + M_{\frac{p-1}{d}-1}(10^0 + 10^d + \dots + 10^{p-1-d})$$

égal à

$$(M_1 + \dots + M_{\frac{p-1}{d}-1})(10^0 + 10^d + \dots + 10^{p-1-d})$$

égal à

$$(M_1 + \dots + M_{\frac{p-1}{d}-1}) \frac{10^{p-1} - 1}{10^d - 1}$$

Finalement :

$$(M_1 + \dots + M_{\frac{p-1}{d}-1}) \frac{10^{p-1} - 1}{10^d - 1} = n \times (10^{p-1} - 1)$$

Donc

$$M_1 + \dots + M_{\frac{p-1}{d}-1} = n \times (10^d - 1)$$

Quatrième partie

La conjecture d'Artin

12 Énoncé de la conjecture

En 1927, Emil Artin conjecture que les nombres premiers longs sont infinis et que leur densité parmi les nombres premiers est :

$$C_{artin} = \prod_{p \in \mathcal{P}} 1 - \frac{1}{p(p-1)}$$

13 Un début de preuve de l'infinité des nombres premiers longs

On doit à Chebyshev cette preuve incomplète qu'il existe une infinité de nombres premiers longs, elle utilise la loi de réciprocité quadratique qu'on doit donc ici introduire.

On définit le symbole de Legendre ainsi : pour p premier, $\left(\frac{a}{p}\right)$ est égal à 1 si a est un carré dans $\mathbb{Z}/p\mathbb{Z}$ (c'est à dire il existe x tel que $a \equiv x^2(p)$) et -1 sinon. On admet les formules :

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(p)$$

$$\left(\frac{a \times b}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}(p)$$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

Si q est un nombre premier tel que $q = 4p + 1$ avec p premier et $p \equiv 2(5)$ alors q est un nombre premier long. En effet :

$$10^{2p} \equiv 10^{\frac{q-1}{2}} \equiv \left(\frac{10}{q}\right) \equiv \left(\frac{2}{q}\right) \left(\frac{5}{q}\right) \equiv (-1)^{\frac{q^2-1}{8}} \left(\frac{q}{5}\right) \equiv -\left(\frac{9}{5}\right) \equiv -\left(\frac{2^2}{5}\right) \equiv -1(q)$$

L'ordre de 10 est un diviseur de $q - 1 = 4p$ (donc 1, 2, 4, p , $2p$ ou $4p$) or $10^{2p} \equiv -1(p)$ donc l'ordre de 10 ne peut être p ou $2p$, de plus on remarque que $10^4 - 1 = 3^2 \times 11 \times 101$ et 3, 11, 101 ne peuvent être q donc l'ordre de 10 est différent de 1, 2 ou 4. Finalement l'ordre de 10 est $4p$ donc 10 est une racine primitive et q est un nombre premier long.

Si l'on suppose qu'il existe une infinité de nombres premiers de cette forme alors il y a une infinité de nombres premiers longs.

14 Probabilités

Soit q et p deux nombres premiers, 10 n'est pas une racine primitive modulo p si q divise $p - 1$ et $10^{\frac{p-1}{q}} \equiv 1(p)$. Le premier "événement" $p \equiv 1(q)$ est vrai pour les nombres premiers p avec une fréquence de $\frac{1}{\phi(q)} = \frac{1}{q-1}$ d'après le théorème de Dirichlet (que l'on admet ici biensur). Le second événement est $10^{\frac{p-1}{q}} \equiv 1(p)$ soit l'événement $10^{\frac{p-1}{q}}$ est une solution de l'équation $x^q \equiv 1(p)$ et nous supposons que cette équation possède q solutions, de plus nous savons qu'il y a une solution congru à 1 modulo p (car $x - 1$ divise $x^q - 1$) donc⁵ la probabilité du second événement est $\frac{1}{q}$. Si les deux événements sont indépendants alors la probabilité que les deux événements soient vrais est $\frac{1}{q(q-1)}$. En faisant parcourir q parmi les nombres premiers on obtient la constante d'Artin

$$C_{artin} = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p(p-1)}\right).$$

En fait, au lieu de parcourir les nombres premiers p pour savoir si p a 10 pour racine primitive, on parcourt les nombres premiers q qui permettent de dire qu'il y a des nombres premiers p qui n'ont pas 10 comme racine primitive.

Cette vision probabiliste n'est pas rigoureuse⁶ et elle ne peut faire office de preuve mais elle permet de comprendre la formule de la constante d'artin après que l'on ait bien compris le "rôle" de q dans le raisonnement : $1 - \frac{1}{q(q-1)}$ n'est pas la probabilité pour que q ait 10 pour racine primitive mais la fraction des nombres premiers p dont l'ordre de 10 n'est pas $\frac{p-1}{q}$.

Conclusion

Les nombres têtus sont une curiosité mathématique exceptionnelle, ils sont vraiment très peu connus⁷ pourtant ils possèdent des propriétés vraiment remarquables et finalement ils sont fréquemment⁸ implicitement exprimés lorsque l'on utilise le théorème de Fermat. En revanche, l'étude des racines primitives est bien plus répandue et les résultats d'Emil Artin ou Christopher Hooley sont vraiment intéressants mais trop longs et difficiles pour être présentés ici. On peut peut-être imaginer dans le futur d'utiliser les nombres premiers longs avec le cryptage RSA en utilisant les propriétés du nombre têtu associé pour définir la clé ...

Références

<http://membres.lycos.fr/villemingerard/Nombre/Tetu.htm>

Nombres premiers : mystères et records , Paulo Ribenboim. 1994

Merveilleux nombres premiers : voyage au coeur de l'arithmétique , Jean-Paul Delahaye. 2000

<http://staff.science.uva.nl/moree/Artinober.ps>

<http://mathworld.wolfram.com/MidysTheorem.html>

<http://mathworld.wolfram.com/CyclicNumber.html>

<http://mathworld.wolfram.com/FullReptendPrime.html>

<http://www.mjc-andre.org/pages/amej/labo/sujlab01/inver01c/inverse.html>⁹

⁵Il y a q solutions, la probabilité pour que la solution $10^{\frac{p-1}{q}}$ et la solution congru à 1 modulo p coïncident est donc $q \times \frac{1}{q} \times \frac{1}{q} = \frac{1}{q}$

⁶D'ailleurs Pieter MOREE l'appelle "Naive heuristic approach"

⁷Une recherche sur google donne 37 pages pour 3 sites : l'excellent site de Gérard Villemin (en référence), un article que j'ai publié sur france-jeunes.net, l'atelier Maths en jeans.

⁸Une fréquence de C_{artin}

⁹Je suis l'auteur du premier message de cette page où j'ai répondu au problème correctement mais j'ai dit de grosses bêtises, c'était il y a 3 ans.