Développement décimal de $1/p$ (d'après O. Mathieu)

Besançon, 2 juin 2006

Jérôme Germoni (université Lyon 1)

Plan

Devinettes

Devinettes

1. Calculer de tête le 53-ème chiffre de 1/53.
2. Calculer de tête le 52-ème chiffre de 1/53.
3. Calculer de tête le 27-ème chiffre de 1/53.
4. Julian additionne deux nombres et trouve 999. Combien de retenues a-t-il effectuées ?

Devinettes

Devinettes

1. Calculer de tête le 53-ème chiffre de $1/53$.
2. Calculer de tête le 52-ème chiffre de $1/53$.
3. Calculer de tête le 27-ème chiffre de $1/53$.
4. Julian additionne deux nombres et trouve 999. Combien de retenues a-t-il effectuées ?

Une réponse

4. Si Julian a calculé $142 + 857$, il n'a pas fait de retenue.

Devinettes

Devinettes

1. Calculer de tête le 53-ème chiffre de $1/53$.
2. Calculer de tête le 52-ème chiffre de $1/53$.
3. Calculer de tête le 27-ème chiffre de $1/53$.
4. Julian additionne deux nombres et trouve 999. Combien de retenues a-t-il effectuées ?

Une réponse

4. Si Julian a calculé $142 + 857$, il n'a pas fait de retenue. Donc, par contrat didactique, la réponse est : aucune.

Introduction

$$\frac{1}{7} = 0{,}142\,857\ 142\,857\ 142\,857\ \ldots$$

- Développement cyclique.

Introduction

$$\frac{1}{7} = 0{,}142\,857\ 142\,857\ 142\,857\ \ldots$$

- Développement cyclique.
- Pas de demi-mesure :

$$142 + 857 = 999.$$

Introduction

$$\frac{1}{7} = 0{,}142\,857\ 142\,857\ 142\,857\ \ldots$$

- Développement cyclique.
- Pas de demi-mesure :

$$142 + 857 = 999.$$

- Silence, on tourne !

$$\frac{1}{7} = 0{,}142857\cdots,\ \frac{2}{7} = 0{,}285714\cdots,\ \frac{3}{7} = 0{,}428571\cdots,$$
$$\frac{4}{7} = 0{,}571428\cdots,\ \frac{5}{7} = 0{,}714285\cdots,\ \frac{6}{7} = 0{,}857142\cdots$$

Figures tutélaires

Suivant Gauss, *Disquisitiones arithmeticæ* (1801), on s'intéresse au développement décimal de $1/p$, où p est un nombre premier.

p-ème chiffre

$\frac{p+1}{2}$-ème chiffre

longueur $p-1$

Notation : nombres premiers : $\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$.

Plan

Traduction de l'existence d'une période

Dire que le développement de $1/p$ est périodique de période d, c'est dire qu'il existe des chiffres $a_1, \ldots, a_d \in \{0, \ldots, 9\}$ tels que

$$\frac{1}{p} = \overline{0,\underbrace{a_1 a_2 a_3 \cdots a_d}_{d}\,\underbrace{a_1 a_2 a_3 \cdots a_d}_{d}\,\underbrace{a_1 a_2 a_3 \cdots a_d}_{d}\cdots}.$$

Traduction de l'existence d'une période

Dire que le développement de $1/p$ est périodique de période d, c'est dire qu'il existe des chiffres $a_1, \ldots, a_d \in \{0, \ldots, 9\}$ tels que

$$\frac{1}{p} = \overline{0,\underbrace{a_1 a_2 a_3 \cdots a_d}_{d}\underbrace{a_1 a_2 a_3 \cdots a_d}_{d}\underbrace{a_1 a_2 a_3 \cdots a_d}_{d}\cdots}.$$

Posons $n = \overline{a_1 a_2 \ldots a_d} = \sum_{i=1}^{d} a_i 10^{d-i}$, il vient :

$$10^d \times \frac{1}{p} = \overline{\underbrace{a_1 a_2 a_3 \cdots a_d}_{d}, \underbrace{a_1 a_2 a_3 \cdots a_d}_{d}\cdots} = n + \frac{1}{p} \iff np = 10^d - 1.$$

Traduction de l'existence d'une période

Dire que le développement de $1/p$ est périodique de période d, c'est dire qu'il existe des chiffres $a_1, \ldots, a_d \in \{0, \ldots, 9\}$ tels que

$$\frac{1}{p} = \overline{0,\underbrace{a_1 a_2 a_3 \cdots a_d}_{d}\underbrace{a_1 a_2 a_3 \cdots a_d}_{d}\underbrace{a_1 a_2 a_3 \cdots a_d}_{d}\cdots}.$$

Posons $n = \overline{a_1 a_2 \ldots a_d} = \sum_{i=1}^{d} a_i 10^{d-i}$, il vient :

$$\frac{1}{p} = \sum_{i=1}^{+\infty} \frac{n}{10^{id}} = \frac{10^{-d} n}{1 - 10^{-d}} = \frac{n}{10^d - 1} \iff np = 10^d - 1.$$

Existence d'une période

$$\frac{1}{p} = \overline{0,\underbrace{\quad n \quad}_{d}\underbrace{\quad n \quad}_{d}\cdots} \iff np = 10^d - 1.$$

Existence d'une période

$$\frac{1}{p} = \overline{0,\underbrace{\quad n \quad}_{d}\underbrace{\quad n \quad}_{d}\cdots} \iff np = 10^d - 1.$$

Conséquence

- d = longueur d'une période de $1/p \iff p$ divise $10^d - 1$;

Existence d'une période

$$\frac{1}{p} = \overline{0,\underbrace{\quad n \quad}_{d}\underbrace{\quad n \quad}_{d}\cdots} \iff np = 10^d - 1.$$

Conséquence

- d = longueur d'une période de $1/p \iff p$ divise $10^d - 1$;
- plus petite longueur = ordre de 10 dans $(\mathbb{Z}/p\mathbb{Z})^*$;

Existence d'une période

$$\frac{1}{p} = \overline{0,\underbrace{\quad n \quad}_{d}\underbrace{\quad n \quad}_{d}\cdots} \iff np = 10^d - 1.$$

Conséquence

- d = longueur d'une période de $1/p \iff p$ divise $10^d - 1$;
- plus petite longueur = ordre de 10 dans $(\mathbb{Z}/p\mathbb{Z})^*$;
- longueurs possibles = multiples de cet ordre ;

Existence d'une période

$$\frac{1}{p} = \overline{0,\underbrace{\quad n \quad}_{d}\underbrace{\quad n \quad}_{d}\cdots} \iff np = 10^d - 1.$$

Conséquence

- d = longueur d'une période de $1/p \iff p$ divise $10^d - 1$;
- plus petite longueur = ordre de 10 dans $(\mathbb{Z}/p\mathbb{Z})^*$;
- longueurs possibles = multiples de cet ordre ;
- période de $1/p$: $n = \dfrac{10^d - 1}{p} = \dfrac{99\cdots 9}{p}$.

Arithmétique modulo p

modulo p	complexes
$\mathbb{Z}$, $+$, $\times$	$\mathbb{R}[i]$: polynômes en i
nouvelle règle	
p=0	$i^2+1=0$
nombres obtenus	
$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{C}$
$\{0,1,\ldots,p-1\}$	$a+ib$
"miracle"	
tout "nombre" non nul est inversible	

Arithmétique modulo p

Nombres entiers relatifs, règles usuelles, et de plus :

$$p = 0.$$

Arithmétique modulo p

Nombres entiers relatifs, règles usuelles, et de plus :

$$p = 0.$$

Conséquence : ne restent que p "nombres" :

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}.$$

Arithmétique modulo p

Nombres entiers relatifs, règles usuelles, et de plus :

$$p = 0.$$

Conséquence : ne restent que p "nombres" :

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}.$$

Fait : tout nombre $\neq 0$ est inversible. Exemple modulo 7 :

$$1 \times 1 = 2 \times 4 = 3 \times 5 = 6 \times 6 \ [7].$$

Comme il existe $a < b$ tel que $10^a = 10^b \ [p]$, on a, avec $d = b - a$:

$$10^a(1 - 10^d) = 0 \ [p], \quad \text{d'où} \quad 10^d = 1 \ [p].$$

Petit théorème de Fermat

Lemme

Pour $1 \leq k \leq p-1$, $\binom{p}{k}$ est un multiple de p.

Preuve : $p! = k!\,(p-k)!\binom{p}{k}$ et $\operatorname{pgcd}(p, k!(p-k)!) = 1$.

Petit théorème de Fermat

Lemme

Pour $1 \leq k \leq p-1$, $\binom{p}{k}$ est un multiple de p.

Preuve : $p! = k!\,(p-k)!\binom{p}{k}$ et $\operatorname{pgcd}(p, k!(p-k)!) = 1$.

Conséquence

Pour tout $a \in \{1, \ldots, p-1\}$, $a^{p-1} = 1\ [p]$.

On montre $a^p = a$ par récurrence sur a : évident si $a = 1$,

$$(a+1)^p = a^p + 1 = a + 1.$$

Ordre d'un élément

Ordre de 10 dans $(\mathbb{Z}/p\mathbb{Z})^*$

Pour p premier,

- p divise $10^{p-1}-1$:
- si p divise 10^d-1 et 10^e-1, avec d minimal, alors d divise e.

Premier point : petit théorème de Fermat.
Deux preuves du second point :

1. théorème de Lagrange ;
2. $\mathrm{pgcd}(10^a-1, 10^b-1) = 10^{\mathrm{pgcd}(a,b)}-1$.

Devinette

1. Quel est le 53-ème chiffre de $1/53$?

Réponse

1. C'est le même que le premier : 0.

Algorithme de division

$$\begin{array}{r|l} 999\,999 & 7 \\ \hline & \\ & \end{array}$$

Algorithme de division

999 999	7
49	7
95	

Algorithme de division

$$\begin{array}{rl|l} 999\,999 & & 7 \\ \cline{3-3} \underline{49} & & 57 \\ 95 & & \\ \underline{35} & & \\ 96 & & \end{array}$$

Algorithme de division

$$
\begin{array}{r|l}
999\,999 & 7 \\
\cline{2-2}
\underline{49} & 857 \\
95 & \\
\underline{35} & \\
96 & \\
\underline{56} & \\
94 & \\
\end{array}
$$

Algorithme de division

999 999	7
49	2 857
95	
35	
9 6	
5 6	
94	
14	
98	

Algorithme de division

999 999	7
49	42 857
95	
35	
9 6	
5 6	
94	
14	
98	
28	
7	

Algorithme de division

999 999	7
49	142 857
95	
35	
9 6	
5 6	
94	
14	
98	
28	
7	
7	
0	

Devinette

2. Quel est le 52-ème chiffre de $1/53$?

Réponse

2. C'est 3, car $3 \times 3 = 9$.

$$\begin{array}{r|l} 99\cdots9\,999 & 53 \\ \hline & \end{array}$$

Devinette

2. Quel est le 52-ème chiffre de $1/53$?

Réponse

2. C'est 3, car $3 \times 3 = 9$.

$$\begin{array}{r|l} 99\cdots9\,999 & 53 \\ \underline{159} & \qquad 3 \\ 84 & \end{array}$$

Devinette

2. Quel est le 52-ème chiffre de $1/53$?

Réponse

2. C'est 3, car $3 \times 3 = 9$.

$$\begin{array}{r|l} 99\cdots 9\,999 & 53 \\ \underline{159} & \quad\cdots 3 \\ 84 & \\ \cdots & \end{array}$$

Plan

Dichotomie (exemples)

Ici, on suppose que la plus courte période est de longueur paire.
On peut donc la couper en deux.

Dichotomie (exemples)

Ici, on suppose que la plus courte période est de longueur paire.
On peut donc la couper en deux.
Exemples :

- $\frac{1}{7} = 0,142\,857\cdots$
- $\frac{1}{13} = 0,076\,923\cdots$
- $\frac{1}{11} = 0,0\,9\cdots$

Dichotomie (exemples)

Ici, on suppose que la plus courte période est de longueur paire.
On peut donc la couper en deux.
Exemples :

- $\frac{1}{7} = 0,142\,857\cdots$: $142 + 857 = 999$;
- $\frac{1}{13} = 0,076\,923\cdots$: $76 + 923 = 999$;
- $\frac{1}{11} = 0,0\,9\cdots$: $0 + 9 = 9$...

Ca ne saurait être un hasard !

Dichotomie (formalisation)

Lemme

Supposons que $d = 2e$ soit une longueur de période de $1/p$, mais que e ne soit pas la longueur d'une période :

$$\frac{1}{p} = \overline{0,\underbrace{\underbrace{A}_{e}\underbrace{B}_{e}}_{d=2e}\underbrace{\underbrace{A}_{e}\underbrace{B}_{e}}_{d=2e}\cdots}, \quad 0 \leq A, B < 10^e.$$

Alors,

$$A + B = 10^e - 1 = \underbrace{99\cdots9}_{e \text{ chiffres}}.$$

Preuve

$$\frac{1}{p} = \overline{0,\underbrace{A}_{e}\underbrace{B}_{e}\underbrace{A}_{e}\underbrace{B}_{e}\cdots}, \quad 0 \leq A, B < 10^e$$

permet d'écrire

$$\frac{10^{2e}}{p} = 10^e A + B + \frac{1}{p},$$

puis

$$\frac{10^e + 1}{p} \times (10^e - 1) = 10^e A + B.$$

Modulo $10^e - 1$, il vient :

$$A + B \equiv 0\ [10^e - 1] \quad \text{et} \quad 1 \leq A + B < 2(10^e - 1).$$

Un énoncé surprenant

Théorème (O. Mathieu ?)

Soit $p \geq 11$ un nombre premier :

1. la $(p+1)/2$-ème décimale de $1/p$ est 0 ou 9 ;
2. le fait que ce soit 0 ou 9 ne dépend que de p modulo 40.

$$\frac{1}{p} = 0,\underbrace{\underbrace{\cdots}_{e}\downarrow\underbrace{\cdots}_{e}}_{p-1=2e}\cdots$$

Preuve (premier point)

1. Partie facile.

$$\frac{1}{p} = 0,\underbrace{\underbrace{\cdots A}_{e}\overset{\downarrow}{\underbrace{B\cdots}_{e}}}_{p-1=2e}, \quad \begin{cases} A = B \\ \quad ou \\ A + B = 99\cdots 9. \end{cases}$$

Preuve (premier point)

1. Partie facile.

$$\frac{1}{p} = 0,\underbrace{\underbrace{0}_{e}\underbrace{A}_{e}\underbrace{B}_{e}\cdots}_{p-1=2e}, \quad \begin{cases} A = B \\ \quad ou \\ A + B = 99\cdots9. \end{cases}$$

- Cas $A = B$: c'est 0.
- Cas $A + B = 99\cdots9$: c'est 9. En effet :

$$\begin{array}{r} 0\ \bullet\ \cdots\ \bullet\ \bullet \\ +\ ?\ \bullet\ \cdots\ \bullet\ \bullet \\ \hline 9\ 9\ \cdots\ 9\ 9 \end{array} \qquad \begin{array}{r} A \\ +\ B \\ \hline 10^{p-1}-1 \end{array}$$

Preuve (premier point)

1. Partie facile.

$$\frac{1}{p} = 0,\underbrace{\underbrace{\overset{\downarrow}{0}\qquad A}_{e}\underbrace{\overset{\downarrow}{\qquad}\qquad B}_{e}}_{p-1=2e}\cdots, \qquad \begin{cases} A = B \\ \quad ou \\ A + B = 99\cdots 9. \end{cases}$$

   - Cas $A = B$: c'est 0.
   - Cas $A + B = 99\cdots 9$: c'est 9. En effet :

$$\begin{array}{r} 0\ \bullet\ \cdots\ \bullet\ \bullet \\ +\ ?\ \bullet\ \cdots\ \bullet\ \bullet \\ \hline 9\ 9\ \cdots\ 9\ 9 \end{array} \qquad \begin{array}{r} A \\ +\ B \\ \hline 10^{p-1}-1 \end{array}$$

2. Il faut décider si $\frac{p-1}{2}$ est une période, i.e. si p divise $10^{\frac{p-1}{2}} - 1$.

Carrés de $(\mathbb{Z}/p\mathbb{Z})^*$

Lemme

Considérons les carrés : $\{x^2,\ x \in (\mathbb{Z}/p\mathbb{Z})^*\}$.
Un élément $a \in (\mathbb{Z}/p\mathbb{Z})^*$ est un carré SSI $a^{\frac{p-1}{2}} = 1\ [p]$.

Si $a = x^2$, alors, par Fermat, $a^{\frac{p-1}{2}} = x^{p-1} = 1\ [p]$.
La réciproque demande un peu plus de soin.

Exemple ($p = 7$) : carrés : $1^2 = 6^2 = 1$, $2^2 = 5^2 = 4$, $3^2 = 4^2 = 2$.
D'une part, $10 = 3$ n'est pas un carré modulo 7.
D'autre part, 7 ne divise pas $10^{\frac{7-1}{2}} - 1 = 999 = 3^3 \times 37$.

Symbole de Legendre

Notation

Pour p premier et $a \in (\mathbb{Z}/p\mathbb{Z})^*$,

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } (\mathbb{Z}/p\mathbb{Z})^* \\ -1 & \text{sinon.} \end{cases}$$

Justification : $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} = 1$.

Exemple (non trivial)

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p = \pm 1\ [8] \\ -1 & \text{si } p = \pm 3\ [8]. \end{cases}$$

Ce symbole ne dépend donc que de p modulo 8.

Loi de réciprocité quadratique

Théorème (Gauss – 1801)

Soit p, q premiers impairs distincts. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Loi de réciprocité quadratique

Théorème (Gauss – 1801)

Soit p, q premiers impairs distincts. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Application au $(p+1)/2$-ème chiffre : 0 ou 9 ?

La $\frac{p+1}{2}$-ème décimale de $1/p$ est 0 SSI $\left(\frac{10}{p}\right) = 10^{\frac{p-1}{2}} = 1\ [p]$. Or...

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{5}\right).$$

Par le lemme chinois, ceci ne dépend que de p modulo 40.

Découpage de période en 3, 4 et plus

Maitrisant la dichotomie, tentons de diviser plus !
Exemples :

- $\frac{1}{7} = 0,142\ 857\cdots$
- $\frac{1}{7} = 0,14\ 28\ 57\cdots$
- $\frac{1}{13} = 0,07\ 69\ 23\cdots$

Contre-exemple :

- $\frac{1}{73} = 0{,}01\ 36\ 98\ 63\cdots$

Découpage de période en 3, 4 et plus

Maitrisant la dichotomie, tentons de diviser plus !
Exemples (généraliser) :

- $\frac{1}{7} = 0,142\ 857\cdots$: $142 + 857 = 999$;
- $\frac{1}{7} = 0,14\ 28\ 57\cdots$: $14 + 28 + 57 = 99$;
- $\frac{1}{13} = 0,07\ 69\ 23\cdots$: $7 + 69 + 23 = 99$.

Contre-exemple (trouver un énoncé quand même) :

- $\frac{1}{73} = 0{,}01\ 36\ 98\ 63\cdots$: $1 + 36 + 98 + 63 = 2 \times 99$.

Calcul exotique de 1/13

$$\frac{1}{13} = 0, \bullet\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet \cdots$$

- $7 \times 11 \times 13 = 1001 \implies 13 | 10^6 - 1 = (10^3 + 1)(10^3 - 1)$

Calcul exotique de 1/13

$$\frac{1}{13} = 0,0\bullet\bullet\bullet\bullet\bullet\cdots$$

- $7 \times 11 \times 13 = 1001 \implies 13 | 10^6 - 1 = (10^3+1)(10^3-1)$
- $13 > 10$

Calcul exotique de 1/13

$$\frac{1}{13} = 0,0\bullet\bullet\bullet\bullet 3\cdots$$

- $7 \times 11 \times 13 = 1001 \implies 13 | 10^6 - 1 = (10^3+1)(10^3-1)$
- $13 > 10$
- $3 \times 3 = 9$

Calcul exotique de 1/13

$$\frac{1}{13} = 0,0 \bullet 6\ 9 \bullet 3 \cdots$$

- $7 \times 11 \times 13 = 1001 \implies 13 | 10^6 - 1 = (10^3+1)(10^3-1)$
- $13 > 10$
- $3 \times 3 = 9$
- $$\begin{array}{r} 0\bullet\bullet \\ +\ \bullet\bullet 3 \\ \hline 999 \end{array}$$

Calcul exotique de 1/13

$$\frac{1}{13} = 0,076\ 923\cdots$$

- $7 \times 11 \times 13 = 1001 \implies 13 | 10^6 - 1 = (10^3+1)(10^3-1)$
- $13 > 10$
- $3 \times 3 = 9$
- $$\begin{array}{r} 0\bullet\bullet \\ +\ \bullet\bullet 3 \\ \hline 999 \end{array}$$
- $$\begin{array}{r} 0\bullet \\ +\ 69 \\ +\ \bullet 3 \\ \hline 99 \end{array}$$

Plan

Occuper Julian (8 ans) à la pizzeria

$$1 \times 142857 = 142857\cdots,$$

$$2 \times 142857 = 285714\cdots,$$

$$3 \times 142857 = 428571\cdots,$$

$$4 \times 142857 = 571428\cdots,$$

$$5 \times 142857 = 714285\cdots,$$

$$6 \times 142857 = 857142\cdots$$

Occuper Julian (11 ans) à la pizzeria

$$\frac{1}{7} = 0{,}142857\cdots, \quad \frac{2}{7} = 0{,}285714\cdots, \quad \frac{3}{7} = 0{,}428571\cdots,$$
$$\frac{4}{7} = 0{,}571428\cdots, \quad \frac{5}{7} = 0{,}714285\cdots, \quad \frac{6}{7} = 0{,}857142\cdots$$

Que faire à la pizzeria quand Julian aura 13 ans ?

Que faire à la pizzeria quand Julian aura 13 ans ?

$$\frac{1}{13} = 0{,}076923\cdots, \quad \frac{2}{13} = 0{,}153846\cdots, \quad \frac{3}{13} = 0{,}230769\cdots,$$
$$\frac{4}{13} = 0{,}307692\cdots, \quad \frac{5}{13} = 0{,}384615\cdots, \quad \frac{6}{13} = 0{,}461538\cdots$$
$$\frac{7}{13} = 0{,}538461\cdots, \quad \frac{8}{13} = 0{,}615384\cdots, \quad \frac{9}{13} = 0{,}692307\cdots$$
$$\frac{10}{13} = 0{,}769230\cdots, \quad \frac{11}{13} = 0{,}846153\cdots, \quad \frac{12}{13} = 0{,}923076\cdots$$

Que faire à la pizzeria quand Julian aura 13 ans ?

$$\frac{1}{13} = 0{,}076923\cdots, \quad \frac{2}{13} = 0{,}153846\cdots, \quad \frac{3}{13} = 0{,}230769\cdots,$$
$$\frac{4}{13} = 0{,}307692\cdots, \quad \frac{5}{13} = 0{,}384615\cdots, \quad \frac{6}{13} = 0{,}461538\cdots$$
$$\frac{7}{13} = 0{,}538461\cdots, \quad \frac{8}{13} = 0{,}615384\cdots, \quad \frac{9}{13} = 0{,}692307\cdots$$
$$\frac{10}{13} = 0{,}769230\cdots, \quad \frac{11}{13} = 0{,}846153\cdots, \quad \frac{12}{13} = 0{,}923076\cdots$$

Pour $\frac{1}{13}$: nombre de périodes : 2, longueur des périodes : 6.

Proposition

$$\left(\begin{array}{c}\text{nombre de périodes de } k/p \\ (1 \leq k \leq p-1) \\ \text{à permutation cyclique près}\end{array}\right) \times \left(\begin{array}{c}\text{longueur minimale} \\ \text{d'une période}\end{array}\right) = p-1$$

Question

Pour quels nombres premiers a-t-on

- 10 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$;
- la longueur minimale des périodes égale à $p-1$?
- une seule période (à permutation cyclique près) pour tous les k/p, $1 \leq k \leq p-1$;

(Les trois conditions sont équivalentes !)

Deux types de nombres premiers

Pour un nombre premier p, deux cas :

- longueur minimale période $= p - 1$; ex. : $\frac{1}{7} = 0,142857\cdots$;
- longueur minimale période $< p - 1$; ex. : $\frac{1}{13} = 0,076923\cdots$.

Problème

On note

$$\mathcal{P}(10) = \{p \text{ premier: longueur minimale période} = p - 1\}.$$

Deux types de nombres premiers

Pour un nombre premier p, deux cas :

- longueur minimale période $= p-1$; ex. : $\frac{1}{7} = 0,142857\cdots$;
- longueur minimale période $< p-1$; ex. : $\frac{1}{13} = 0,076923\cdots$.

Problème

On note

$$\mathcal{P}(10) = \{p \text{ premier: longueur minimale période} = p-1\}.$$

Est-ce que $\mathcal{P}(10)$ est infini ? Estimer la "densité" de $\mathcal{P}_{10}$:

$$d_{10}(x) = \frac{\operatorname{card}\{p \in \mathcal{P}(10), p \leq x\}}{\operatorname{card}\{p \in \mathcal{P}, p \leq x\}} \quad : \quad \lim_{x\to+\infty} d_{10}(x) \ ?$$

Expériences numériques

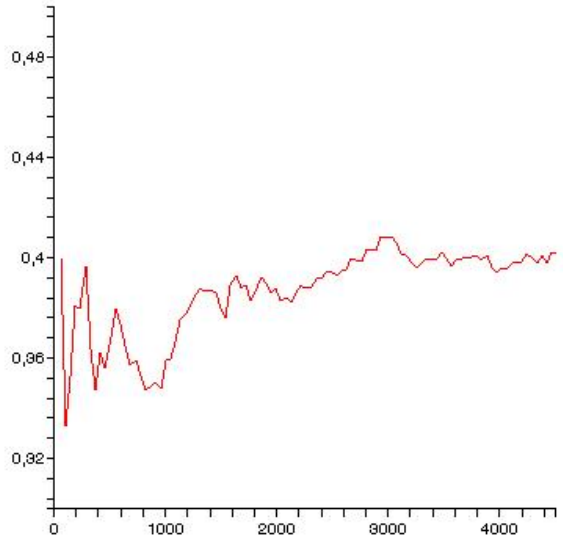
$$\mathcal{P}_{10} = \{7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, \dots\}$$

$$y = d_{10}(x) = \frac{\mathrm{card}\{p \in \mathcal{P}(10), p \leq x\}}{\mathrm{card}\{p \in \mathcal{P}, p \leq x\}}$$

Expériences numériques

$$\mathcal{P}_{10} = \{7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, \dots\}$$

$$y = d_{10}(x) = \frac{\mathrm{card}\{p \in \mathcal{P}(10), p \leq x\}}{\mathrm{card}\{p \in \mathcal{P}, p \leq x\}}$$



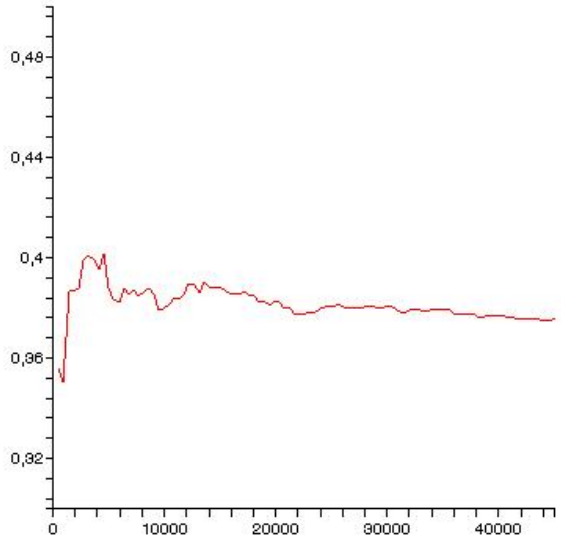
base 10

$x_{\max} = 4500$

Expériences numériques

$$\mathcal{P}_{10} = \{7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, \dots\}$$

$$y = d_{10}(x) = \frac{\mathrm{card}\{p \in \mathcal{P}(10), p \leq x\}}{\mathrm{card}\{p \in \mathcal{P}, p \leq x\}}$$



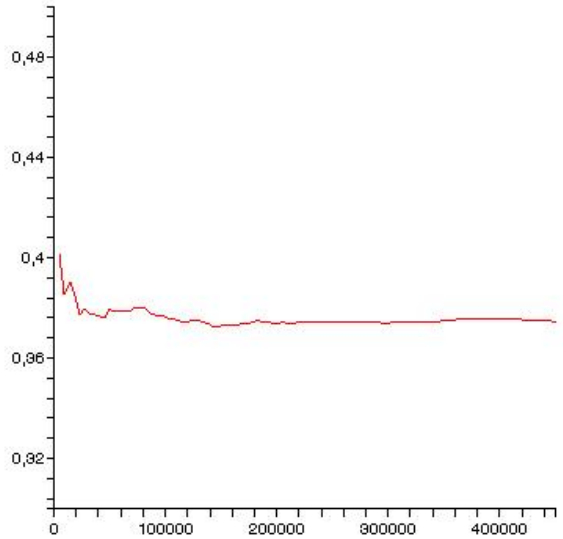
base 10

$x_{\max} = 45000$

Expériences numériques

$$\mathcal{P}_{10} = \{7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, \dots\}$$

$$y = d_{10}(x) = \frac{\mathrm{card}\{p \in \mathcal{P}(10), p \leq x\}}{\mathrm{card}\{p \in \mathcal{P}, p \leq x\}}$$



base 10

$x_{\max} = 450000$

Enoncé de la conjecture (base 10)

Conjecture

- *Il existe un nombre infini de nombres premiers p tels que la plus petite période décimale de $1/p$ soit de longueur $p-1$.*
- *La densité de ces p est :*

$$C_{\text{Artin}} = \prod_{q \text{ premier}} \left(1 - \frac{1}{q(q-1)}\right) \simeq 0{,}373\,955\,813\,6\ldots$$

Remarque : où intervient 10 ?

Expériences numériques : base quelconque

Soit $a \geq 2$ quelconque, pas une puissance d'un entier.

$$\mathcal{P}(a) = \{p \text{ premier}, \ \langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^*\}$$

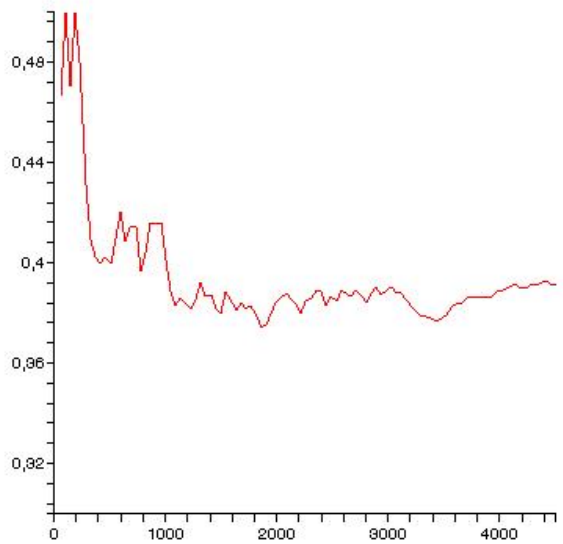
$$d_a(x) = \frac{\mathrm{card}\{p \in \mathcal{P}(a), p \leq x\}}{\mathrm{card}\{p \in \mathcal{P}, p \leq x\}}$$

Expériences numériques : base quelconque

Soit $a \geq 2$ quelconque, pas une puissance d'un entier.

$$\mathcal{P}(a) = \{p \text{ premier}, \ \langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^*\}$$

$$d_a(x) = \frac{\text{card}\{p \in \mathcal{P}(a), p \leq x\}}{\text{card}\{p \in \mathcal{P}, p \leq x\}}$$



$a = 2$

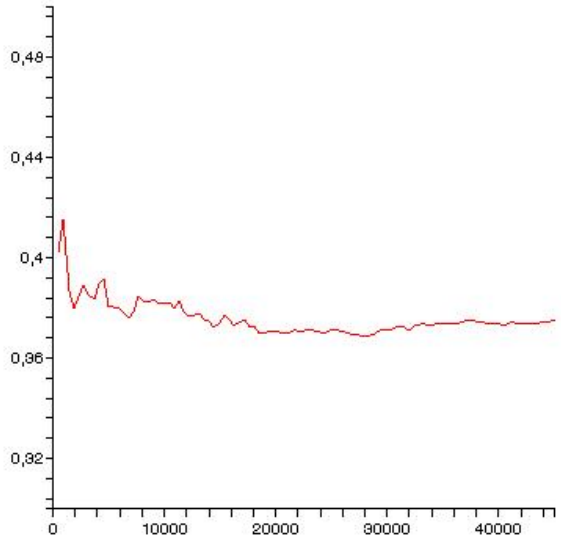
$x_{\max} = 4500$

Expériences numériques : base quelconque

Soit $a \geq 2$ quelconque, pas une puissance d'un entier.

$$\mathcal{P}(a) = \{p \text{ premier}, \ \langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^*\}$$

$$d_a(x) = \frac{\text{card}\{p \in \mathcal{P}(a), p \leq x\}}{\text{card}\{p \in \mathcal{P}, p \leq x\}}$$



$a = 2$

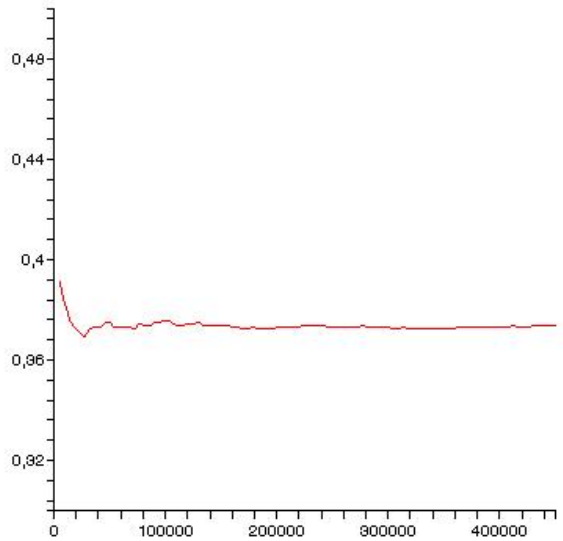
$x_{\max} = 45000$

Expériences numériques : base quelconque

Soit $a \geq 2$ quelconque, pas une puissance d'un entier.

$$\mathcal{P}(a) = \{p \text{ premier}, \ \langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^*\}$$

$$d_a(x) = \frac{\text{card}\{p \in \mathcal{P}(a), p \leq x\}}{\text{card}\{p \in \mathcal{P}, p \leq x\}}$$



$a = 2$

$x_{\max} = 450000$

Enoncé de la conjecture (base presque quelconque)

Conjecture (Artin)

Soit $a \geq 2$, pas une puissance d'un entier.

- Il existe un nombre infini de nombres premiers p tels que la plus petite période du développement de $1/p$ en base a soit de longueur $p-1$.
- La densité de ces p est :

$$C_{\text{Artin}} = \prod_{q \text{ premier}} \left(1 - \frac{1}{q(q-1)}\right) \simeq 0{,}373\,955\,813\,6\ldots$$

Ceci n'est pas une preuve

$$\langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^* \iff \forall q \text{ premier} : \ p \equiv 1\ [q],\ a^{\frac{p-1}{q}} \neq 1\ [p]$$

- Fixons q :
  - probabilité pour que $p = 1\ [q]$: $\dfrac{1}{q-1}$;
  - probabilité pour que $a^{\frac{p-1}{q}} = 1\ [p]$: $\dfrac{1}{q}$.

  Probabilité pour que "ça marche" pour q : $1 - \dfrac{1}{q(q-1)}$.
- Si indépendance, probabilité pour que "ça marche" pour tous les q :

$$\prod_q \left(1 - \frac{1}{q(q-1)}\right).$$

Résultats partiels

- *avec l'hypothèse de Riemann généralisée* (version quantitative) : la conjecture d'Artin est vraie ;
- *résultats inconditionnels* (version qualitative) : au plus 2 ou 3 exceptions parmi les nombres premiers ; par exemple, 2, 3 ou 5 engendrent une infinité de $(\mathbb{Z}/p\mathbb{Z})^*$.