Sur les diviseurs de Fermat
On Fermat's dividers

Méhdi Pascal

Novembre 2020

Abstract :
Fermat's divisors are all integers dividing the polynomial x^n-x, the largest of these divisors is denoted by Z (n) plays an important role in Bernoulli's number theory, it is exactly the denominator of these numbers to one small index shift, for example, whatever the integer x, we have 2730 divided $x^{13}-x$, and b(12)=b(13-1)=-691/2730.
In this paper we will study some properties of these large Fermat divisors.

Résumé :
Les diviseurs de Fermat sont tous entiers divisant le polynôme x^n-x, le plus grand de ces diviseurs est noté par Z(n) joue un rôle important dans la théorie des nombres de Bernoulli, c'est exactement le dénominateur de ces nombres à un petit décalage d'indice, par exemple, quelque soit l'entier x, on a 2730 divise $x^{13}-x$, et b(12)=b(13-1)=-691/2730.
Dans ce papier nous allons étudier quelques propriétés de ces grands diviseurs de Fermat.

Un grand merci à viXra

Sur les diviseurs de Fermat
On Fermat's dividers

À mon neveu Amine Ouzane le physicien de la famille

Sir John H Conway
1937-2020
Mathématicien britannique

Ce présent papier requis les connaissances suivantes :

Les nombres de Bernoulli

Les nombres de Bernoulli sont définis par la fonction génératrice suivante :

$$\frac{x}{e^x-1}=\sum_{n=0}^{+\infty} b_n \frac{x^n}{n!} \qquad |x|<2\pi \ .$$

On a,

$$x=\frac{x}{e^x-1}(e^x-1)=\left(\sum_{n=0}^{+\infty} b_n \frac{x^n}{n!}\right)\left(\sum_{n=1}^{+\infty} \frac{x^n}{n!}\right)=0+1\frac{x}{1!}+0\frac{x^2}{2!}+0\frac{x^3}{3!}+..[]..$$

Et par la règle du produit de Cauchy on obtient la récurrence suivante :

$$\sum_{j=0}^{n-1}\binom{n}{j} b_j=\begin{cases}1 \ si \ n=1\\ 0 \ Ailleurs\end{cases}$$

Les premières valeurs,

n	0	1	2	3	4	5	6	7	8	9	10	11	12
b(n)	1	$\frac{-1}{2}$	$\frac{1}{6}$	0	$\frac{-1}{30}$	0	$\frac{1}{42}$	0	$\frac{-1}{30}$	0	$\frac{5}{66}$	0	$\frac{-691}{2730}$

Cette récurrence permet de prouver que les nombres de Bernoulli sont des rationnels.

Théorème (Von Staudt Clausen)

$$\left(b_n+\sum_{\substack{p,premier\\ p-1|n}}\frac{1}{p}\right)\in\mathbb{Z}$$

Admet.

Une conséquence immédiate de ce théorème est :

$$b_n=\frac{Num(n)}{Dén(n)} \quad \text{avec} \quad Dén(n)=\prod_{\substack{p,premier\\ p-1|n}} p \ .$$

Le petit théorème de Fermat

Théorème (Fermat)

Pour tout $x\in\mathbb{N}$, et pour tout entier n≥2 on a,

Si *n* est premier alors $n|x^n-x$.

Inversement un entier composé *n* qui vérifie cette proposition est dit nombre de Carmichael, qu'on peut l'obtenir par le critère de Korselt, tel que :

Théorème (Critère de Korselt)

Soit n un entier composé, les conditions suivantes sont équivalentes,

- n est un nombre de Carmichael.
- n est impair, sans facteur carré et, pour tout facteur premier p de n, p-1 divise n-1.

[]

Il est clair qu'un nombre de Carmichael est composé au moins de trois facteurs premiers.

Les nombres de Sophie Germain

Un entier s est un nombre de Sophie Germain, si s est premier et tel que 2s+1 est aussi premier.

Le nombre 2s+1 est dit le sûr.

La règle du produit de Cauchy

Pour deux séries ordinaires, on a formellement,

$$\left(\sum_{n\geq 0} a_n x^n\right)\left(\sum_{n\geq 0} b_n x^n\right)=\sum_{n\geq 0} c_n x^n$$

Avec,

$$c_n=\sum_{j=0}^{n} a_j b_{n-j}$$

On remplace a_n par $\frac{a_n}{n!}$, et b_n par $\frac{b_n}{n!}$, donc $c_n=\sum_{j=0}^{n}\frac{a_j}{j!}\frac{b_{n-j}}{(n-j)!}=\sum_{j=0}^{n}\frac{1}{n!}\binom{n}{j}a_j b_{n-j}$

Ainsi,

$$\left(\sum_{n\geq 0} a_n \frac{x^n}{n!}\right)\left(\sum_{n\geq 0} b_n \frac{x^n}{n!}\right)=\sum_{n\geq 0} c_n \frac{x^n}{n!}$$

Avec,

$$c_n=\sum_{j=0}^{n}\binom{n}{j}a_j b_{n-j}$$

[]

Pour les démonstrations de ce requis, WikipédiA suffit, pour la démonstration du théorème de Von Staudt Clausen, la plus simple est disponible en [1], une variété des démos est disponible en [2].

Définition (1) :

Soit $F_n(x)=x^n-x$ la suite de polynôme de Fermat, un entier $a\geq2$ est dit diviseur de Fermat d'ordre $n\geq2$ si quelque soit l'entier x, a divise $F_n(x)=x^n-x$.

Exemples :

- 2 est un diviseur de Fermat d'ordre n quelconque.
- 6 est un diviseur de Fermat de tout ordre impair excepté 1.
- Un nombres premier ou un nombre de Carmichael est un diviseur de Fermat d'ordre lui même.

Théorème (2) :

Un diviseur de Fermat d'ordre $n\geq2$ est un entier $a\geq2$ sans facteur carré, et tel que, pour tout facteur premier p de a, on a $p-1$ divise $n-1$.

Preuve :

Il est facile d'obtenir la formule suivante :

(3) :
$$\left(x^q-1\right)=\left(x^p-1\right).\sum_{j=1}^{j=s}x^{q-jp}+R(x)$$

Avec $q=sp+r$ et $R(x)=x^r-1$

En vertu de (3) on a,

(4) : $\forall p\in\mathbb{N}^*$ et $\forall q\in\mathbb{N}$ on a, $p|q$ si et seulement si $(x^p-1)\,|\,(x^q-1)$.

On déduit que $F_m(x)$ divise $F_n(x)$ pour tout entier x, si et seulement si $m-1$ divise $n-1$.

Exemple :

$$(x^{13}-x)=(x^4-x)\,(x^9+x^6+x^3+1)$$

Ainsi si $n-1=k(m-1)$ alors on a,

(5) :
$$F_n(x)=F_m(x)\cdot g(x)$$

Avec $g(x)=\sum_{j=1}^{k}x^{(n-1)-j(m-1)}$.

Donc si m est un nombre premier, alors m divise $F_m(x)$, et donc il divise $F_n(x)$.

Si $m=p^2$ avec p est premier, alors on a, d'un part m ne peut pas diviser $g(x)$, il suffit de donner à x la valeur 0 « $g(0)=1$ », d'autre part m ne peut pas diviser (x^m-x), par le critère de Korselt, car $m=p^2$ n'est ni un nombre premier ni un nombre de Carmichael.

C.Q.F.D

Notons aussi par :

(6) :
$$Z_n=\prod_{\substack{p,\,premier\\ p-1|n-1}}p$$

De (1) et (2), il est claire que le nombre Z_n n'est que le plus grand diviseur de Fermat d'ordre $n\geq2$ quelconque.

Ainsi on a :

(7) : pour tout entier x et tout entier n≥2 $x^n \equiv x \ \ Modulo(Z_n)$.

Premiers valeurs :

$$Z_2 = Z_{2n} = 2$$
$$Z_3 = 6$$
$$Z_5 = 30$$
$$Z_7 = 42$$
$$Z_9 = 30$$
$$Z_{11} = 66$$
$$Z_{13} = 2730$$

..[]..

Par convention on pose $Z_1=1$.
Ce plus grand diviseur de Fermat apparaît dans plusieurs classes des polynômes, est non seulement dans la classe de Fermat, mais le plus important c'est il fait partie des fameux nombres de Bernoulli, est plus précisément c'est le dénominateur de ces nombres avec un petit décalage d'indice, comme des fractions on note souvent les nombres de Bernoulli par,

(8) : $$B_n = \frac{N_n}{D_n}$$

Et on a,

(9) : $$D_n = Z_{n+1} = \prod_{\substack{p,\, premier \\ p-1|n}} p$$

Voici quelques propriétés de Z_n.
Dans la suite de ce document p dénote un nombre premier.

(10) : Pour tout entier n, Z(2n)=2, car 2n-1 est impaire, alors que p-1 est pair sauf si p=2.

(11) : 2 divise Z(n) pour tout n ≥ 2, car x^n et x ont la même parité.

(12) : 3 divise Z(n) pour tout n impair ≥ 3, car 2=3-1 divise n-1.

(13) : Z(n) est un entier sans facteur carré , déjà vu.

(14) : n divise Z(n) si et seulement si n est un nombre premier ou n est un nombre de Carmichael ou n=1.
En effet, c'est évident dans le sens où n est un nombre premier ou un nombre de Carmichael, dans l'autre sens, si n|Z(n) alors on a,

- Si n est pair alors n=2.
- Si n est produit seulement de deux nombres premiers impairs alors n est un carré, car l'un de ces deux nombres premiers divisera l'autre, ce qu'est impossible, puisque Z(n) est sans facteur carré. Et en effet, on pose n=pq, où p et q sont premiers, d'après la définition de Z(n) on a, p-1|n-1 & q-1|n-1, or n-1=pq-1=(p-1)q+q-1, puisque p-1|n-1 donc p-1 divise aussi q-1, de même raisonnement on trouve q-1|p-1, donc p=q.
- 1|Z(1)=1 c'est juste par convention.

(15) : Soit p un nombre premier, si $p|Z(n)$, alors $p|Z(n+k(n-1))$ pour tout entier k.

En effet, soit p un nombre premier qui divise Z(n), donc $p-1|n-1$, il divise aussi $(n-1+k(n-1))$, donc il divise $Z(n+k(n-1))$.
Exemple, si on pose $k=(n^a-n)/(n-1)$ qu'est bien un entier, en déduit que si p divise Z(n), alors p divise $Z(n^a)$, pour tout entier a non nul.

Notons par $\wp$ l'ensemble des Z(n), $\wp=\{2,6,30,42,66,138,282,330,354,498,..[]..\}$
La suite A090801 dans OEIS.
La question qui se pose est, quelle est la structure de cet ensemble ? Par exemple, pour quoi 102 n'est pas un élément de $\wp$? Il est très difficile de démontrer que cet ensemble est infini, par exemple on a,

(16) : L'infinité des nombres premiers de Sophie Germain[1] implique l'infinité de $\wp$.
Car si $p\geq 3$ est un nombre de Sophie Germain, et $s=2p+1$ son sûr, alors $Z(s)=6s$.

Et pourtant on peut démontrer que pour chaque $Z(n)=Q$, il existe une infinité des n, c'est évident pour $Z(n)=2$, car $Z(2k)=2$ pour tout entier K, avec de plus la densité qui vaut 1/2.

Pour $Z(n)=6$, on a, si p est un nombre premier de la forme 3k+1, alors $Z(2p+1)=6$, en effet, les diviseurs 2p sont : 1,2,p & 2p, les nombres qui sont candidats d'être des facteurs premiers de $Z(2p+1)$ sont 2,3,p+1 & 2p+1, dont seulement 2 et 3 sont premiers.

Pour $Z(n)=30$, on a, si p est un nombre premier de la forme 15k+1, alors $Z(4p+1)=30$, en effet, les diviseurs de 4p sont, 1,2,4,p,2p et 4p, les candidats sont 2,3,5,p+1,2p+1 et 4p+1, dont seulement 2,3 et 5 sont premiers.

Pour $Z(n)=42$, on a, si p est un nombre premier de la forme 21k+1, alors $Z(6p+1)=42$, en effet, les diviseurs de 6p sont, 1,2,3,6,p,2p,3p et 6p, et les candidats sont 2,3,4,7,p+1,2p+1,3p+1 et 6p+1, dont seulement 2,3 et 7 sont premiers.

Pour le cas générale, en fait la même démarche, telle que,

(17) : Soit Q un entier, tel que $Z(n)=2Q$, et k le plus petit entier tel que $Z(2k+1)=2Q$, l'infinité des entiers n tels que $Z(n)=2Q$ est due à la proposition suivante :
Si p est un nombre premier de la forme Qn+1, alors $Z(2kp+1)=2Q$.

Exemple :
$Z(n)=1770$, $Q=885$, $2k=116=2.2.29$, soit p un nombre premier de la forme 885n+1, et on a les diviseurs de 2kp sont, 1,2,4,29,58,116,p,2p,4p, 29p,58p,116p, les candidats sont 2,3,5,30,59,117,p+1,2p+1,4p+1,29p+1,58p+1 et 116p+1 et on a :

2 divise p+1
3 divise 2p+1=1770n+3
5 divise 4p+1=3540n+5
5 divise 29p+1=25665n+30
59 divise 58p+1=51330n+59

[1] Sophie Germain est une mathématicienne physicienne et philosophe française, 1776-1831.
Un nombre premier p est dit un nombre de Sophie Germain si 2p+1 est aussi un nombre premier, par exemple 2, 3, 5, 11, 23, 29..[].. le nombre 2p+1 est dit le sûr de p.

3 divise 116p+1=102660n+117

Donc parmi tous ces candidats, seuls 2, 3, 5 et 59 sont premiers, dont le produit vaut à 1770.

Pour la densité, d'après le site d'Eric Weisstein, « http:\\mathworld.wolfram.com\BernoulliNumber.html » PAUL ERDOS AND SAMUEL S. WAGSTAFF ont démontrés que les entiers k dont D(2k)=6 vaut à 1/6, donc la densité des entiers n tels que Z(n)=6 vaut à 1/12, car d'un part Z(n)=D(n-1), c'est justifier par le théorème de Von Staudt Clausen, et d'autre part en ne compte pas les D(2k+1), puisque les nombres de Bernoulli sont nuls pour les ordres impairs sauf pour n=1, alors que pour les grands diviseurs de Fermat on compte les Z(2n).
D'après le même auteur, Simon Plouffe a fait une vérification numérique jusqu'à B(5 285 000), il a trouver que cette densité vaut à 0,1526…

La question qui se pose est : Quelle est la structure des entiers n dont Z(n)=6 ?

On trouve la moitié de la réponse chez André Joyal, tel que si p est un nombre premier, et 2p+1 est composé, alors Z(2p+1)=6, facile à démontrer, mais il est important de signaler que si n est composé tel que Z(2n+1)=6, alors pour tout p premier qui divise n on a 2p+1 est composé, en effet supposons que p est un nombre premier de Sophie Germain qui divise n, et que Z(2n+1)=6, alors parmi les diviseurs de 2n on a 1, 2 & 2p, donc parmi les candidats on a 2, 3 & 2p+1, et donc 2*3*(2p+1)=12p+6>6 est un diviseur de Z(2n+1), ce qu'est absurde.
L'inverse n'est pas toujours vrai, par exemple n=7.17=119, « 7 et 17 ne sont pas des nombres de Sophie Germain » et on a Z(2n+1)=Z(239)=1434.
Ceci se résume comme suivant :
Soit,

$$\mathbb{L}_6 = \begin{Bmatrix} p \;\; est \;\; premier \\ 2p+1 \;\; est \;\; composé \end{Bmatrix}$$

$\mathbb{L}_6$ est l'ensemble de tous les nombres premiers excepté les nombres de Sophie Germain.

Si Z(2n+1)=6 alors pour tout premier p qui divise n on a p$\in \mathbb{L}_6$.

Pour la structure des entiers n dont Z(n)=30, on a ce petit théorème, tel que soit p un nombre premier, dont 2p+1 et 4p+1 sont composés, alors Z(4p+1)=30, facile à démontrer, de même il aisé par absurde de prouver le suivant :
Soit,

$$\mathbb{L}_{30} = \begin{Bmatrix} p \;\; est \;\; premier \\ 2p+1 \;\; est \;\; composé \\ 4p+1 \;\; est \;\; composé \end{Bmatrix}$$

Si Z(4n+1)=30 alors pour tout premier p qui divise n on a p$\in \mathbb{L}_{30}$.

De même pour la structure des entiers n dont Z(n)=42, on a,

$$\mathbb{L}_{42} = \begin{Bmatrix} p \;\; est \;\; premier \\ 2p+1 \;\; est \;\; composé \\ 6p+1 \;\; est \;\; composé \end{Bmatrix}$$

Si Z(6n+1)=42 alors pour tout premier p qui divise n on a p$\in \mathbb{L}_{42}$.

Plus généralement, pour déterminer la structure des entiers n dont Z(n)=Q, on se procède comme suivant :
(18) :
Soit k le plus petit entier tel que Z(2k+1)=Q∈$\wp$, soient $d_1=2, d_2, ..[].. d_n$ les diviseurs pairs de 2k, alors on a :

$$\mathbb{L}_Q = \begin{Bmatrix} p \;\; est \;\; premier \\ 2p+1 \;\; est \;\; composé \\ d_2 p+1 \;\; est \;\; composé \\ ..[].. \\ d_n p+1 \;\; est \;\; composé \end{Bmatrix}$$

Et on a,

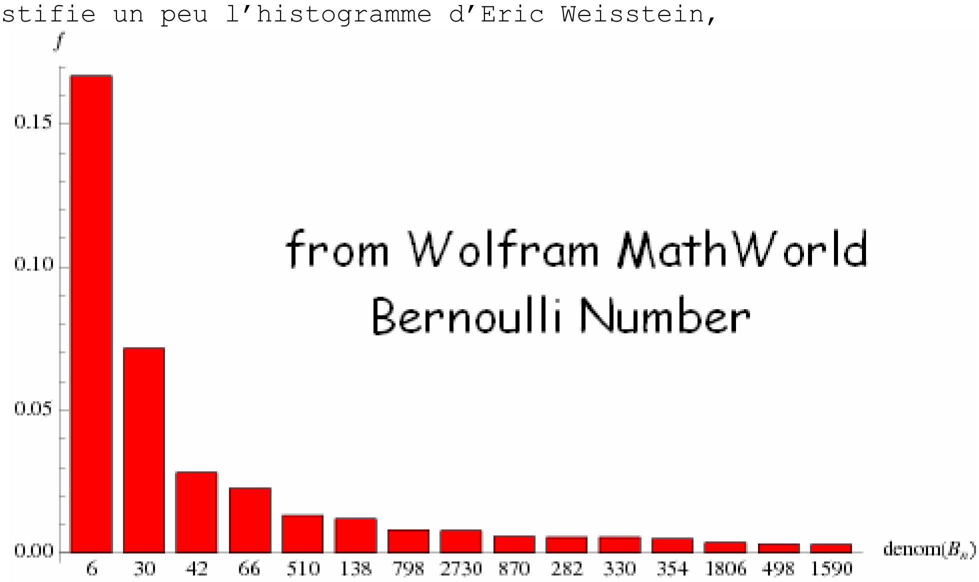
Pour tout premier p de $\mathbb{L}_Q$, Z(2kp+1)=Q, et de plus,

Si Z(2kn+1)=Q alors pour tout premier p divisant n on a p∈$\mathbb{L}_Q$.

Exemple :
Q=330, 2k=20, les diviseurs pairs de 2k sont : 2, 4, 10 et 20, donc,

$$\mathbb{L}_{330} = \begin{Bmatrix} p \;\; est \;\; premier \\ 2p+1 \;\; est \;\; composé \\ 4p+1 \;\; est \;\; composé \\ 10p+1 \;\; est \;\; composé \\ 20p+1 \;\; est \;\; composé \end{Bmatrix}$$

Ceci justifie un peu l'histogramme d'Eric Weisstein,



Il est claire que le domaine $\mathbb{L}_6$ est le plus dominant, car $\forall Q \in \wp$ on a $\mathbb{L}_Q \subset \mathbb{L}_6$, et pour comprendre pour quoi le domaine $\mathbb{L}_{30}$ est plus dominant que $\mathbb{L}_{42}$, il suffit de comparer la densité des nombres premiers de chaque domaine, et on a :

$$\mathbb{L}_{30}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 4p+1 \ \ est \ \ composé \end{Bmatrix}, \quad \mathbb{L}_{42}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 6p+1 \ \ est \ \ composé \end{Bmatrix}$$

Pour $\mathbb{L}_{30}$ les 4 progressions arithmétiques suivantes 4p, 4p+1, 4p+2 et 4p+3 partagent ensemble tous les entiers lorsque p est pris comme un entier quelconque et non premier, les deux progressions 4p et 4p+2 sont composées, en vertu la densité des nombres composés dans la progression 4p+1 est moindre de 1/4, car les progression 4p+1 et 4p+3 contient chaque une infinité des nombres premiers.

De même pour $\mathbb{L}_{42}$ la densité des nombres composés dans la progression 6p+1 est moindre de 1/6, ce qui justifier que le domaine $\mathbb{L}_{30}$ est plus dominant que $\mathbb{L}_{42}$.

Voici la liste des domaines relatifs au diagramme d'Eric Weisstein.

$$\mathbb{L}_{6}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \end{Bmatrix} \quad \mathbb{L}_{30}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 4p+1 \ \ est \ \ composé \end{Bmatrix} \quad \mathbb{L}_{42}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 6p+1 \ \ est \ \ composé \end{Bmatrix}$$

$$\mathbb{L}_{66}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 10p+1 \ \ est \ \ composé \end{Bmatrix} \quad \mathbb{L}_{510}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 4p+1 \ \ est \ \ composé \\ 8p+1 \ \ est \ \ composé \\ 16p+1 \ \ est \ \ composé \end{Bmatrix}$$

$$\mathbb{L}_{138}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 22p+1 \ \ est \ \ composé \end{Bmatrix} \quad \mathbb{L}_{798}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 6p+1 \ \ est \ \ composé \\ 18p+1 \ \ est \ \ composé \end{Bmatrix}$$

$$\mathbb{L}_{2730}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 4p+1 \ \ est \ \ composé \\ 6p+1 \ \ est \ \ composé \\ 12p+1 \ \ est \ \ composé \end{Bmatrix} \quad \mathbb{L}_{870}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 4p+1 \ \ est \ \ composé \\ 14p+1 \ \ est \ \ composé \\ 28p+1 \ \ est \ \ composé \end{Bmatrix}$$

$$\mathbb{L}_{282}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 46p+1 \ \ est \ \ composé \end{Bmatrix} \quad \mathbb{L}_{330}=\begin{Bmatrix} p \ \ est \ \ premier \\ 2p+1 \ \ est \ \ composé \\ 4p+1 \ \ est \ \ composé \\ 10p+1 \ \ est \ \ composé \\ 20p+1 \ \ est \ \ composé \end{Bmatrix}$$

$$\mathbb{L}_{354} = \begin{Bmatrix} p \;\; est \;\; premier \\ 2p+1 \;\; est \;\; composé \\ 58p+1 \;\; est \;\; composé \end{Bmatrix} \qquad \mathbb{L}_{1806} = \begin{Bmatrix} p \;\; est \;\; premier \\ 2p+1 \;\; est \;\; composé \\ 6p+1 \;\; est \;\; composé \\ 14p+1 \;\; est \;\; composé \\ 42p+1 \;\; est \;\; composé \end{Bmatrix}$$

$$\mathbb{L}_{498} = \begin{Bmatrix} p \;\; est \;\; premier \\ 2p+1 \;\; est \;\; composé \\ 82p+1 \;\; est \;\; composé \end{Bmatrix} \qquad \mathbb{L}_{1590} = \begin{Bmatrix} p \;\; est \;\; premier \\ 2p+1 \;\; est \;\; composé \\ 4p+1 \;\; est \;\; composé \\ 26p+1 \;\; est \;\; composé \\ 52p+1 \;\; est \;\; composé \end{Bmatrix}$$

[]

Une identité de Bernd C.Kellner (19) :

$D_{2n} = 2n$, si et seulement si 2n=1806

Z(n) et les diophantes

Théorème (20) :

Soit, $(E) := \sum_{j=1}^{t} a_j x_j^n = 0 \quad a_j \in \mathbb{Z}$, n et t quelconques, et soit $\beta = \sum_{j=1}^{n} a_j x_j$.

Si (E) est soluble, alors $\beta \equiv 0 \;\; Modulo(Z_n)$.

Preuve :

En effet, d'après (7) on a : $\sum_{j=1}^{t} a_j x_j^n - \sum_{j=1}^{t} a_j x_j \equiv 0 \;\; Modulo(Z_n)$,

donc $-\beta \equiv -\sum_{j=1}^{t} a_j x_j \equiv 0 \;\; Modulo(Z_n)$.

C.Q.F.D

Par exemples on a :

$$1^3+5^3+9^3=7^3+8^3$$
$$3^4+21^4+23^4=1^4+4^4+17^4+25^4$$
$$5^5+8^5+13^5+14^5=1^5+6^5+7^5+11^5+15^5$$
$$5^6+15^6+16^6+19^6+22^6=1^6+4^6+13^6+18^6+20^6+21^6$$
$$3^7+6^7+16^7+18^7+22^7+28^7=1^7+2^7+7^7+11^7+21^7+24^7+27^7$$

Dans tous ces exemples, l'égalité est préserver lorsque on supprime les puissances, cela veut dire que β=0, donc β≡0 Modulo(Z(n)).

Z(n) et les polynômes

Soit le symbole suivant :

(21) : $$\underset{x,y\in\mathbb{N}^*}{\delta x,y} = \begin{cases} 1, \text{ Si } (x,y)=1 \\ 0, \text{ Sinon} \end{cases}$$

Ce symbole n'est autre que le caractère trivial de Dirichlet, et comme tout caractère de Dirichlet il est périodique comme il montre le tableau suivant :

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
y=1	**1**	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y=2	**1**	**0**	1	0	1	0	1	0	1	0	1	0	1	0	1
y=3	**1**	**1**	**0**	1	1	0	1	1	0	1	1	0	1	1	0
y=4	**1**	**0**	1	0	1	0	1	0	1	0	1	0	1	0	1
y=5	**1**	**1**	**1**	**1**	**0**	1	1	1	1	0	1	1	1	1	0
y=6	**1**	**0**	**0**	**0**	**1**	**0**	1	0	0	0	1	0	1	0	0
y=7	**1**	**1**	**1**	**1**	**1**	**1**	**0**	1	1	1	1	1	1	0	1

On peut introduire ce symbole pour donner une nouvelle forme au PTF, que j'appelle la forme logique de petit théorème de Fermat, tel que :

La forme logique du petit théorème de Fermat (22) :

Pour tous x,p de ℕ* on a :

Si p est premier alors $x^{p-1} \equiv \delta(x,p)$ Modulo (p).

Preuve :

Soient p un nombre premier, et pour tout entier x, on a :

- Si (x,p)=1, alors c'est le petit théorème de Fermat, tel que, $x^{p-1}\equiv 1$ Modulo (p)
- Si (x,p)≠1, alors (x,p)=p, puisque p est premier, donc p divise x, et évidemment il divise toutes les puissances de x, en particulier x^{p-1}, d'où $x^{p-1}\equiv 0$ Modulo (p).

C.Q.F.D

Comme exemple d'application de cette forme, je propose la proposition suivante :

Proposition (23) :

Si n+1 est premier, et que l'équation $x^n + y^n = z^n$ est soluble par entiers non nuls, alors l'un des deux indéterminés x ou y est forcement multiple de n+1

Preuve :

En effet, une table logique au caractère trivial de Dirichlet est suffisante, telle que :

$\delta_{x,n+1}$	$\delta_{y,n+1}$	$\delta_{z,n+1}$	
0	0	0	n+1 est un diviseur commun
1	0	1	Vrai, donc possible
0	1	1	Vrai, donc possible
1	1	2	Faux, donc impossible

Pour cette raison, lorsque 3 divise z pour le cas de n=2, alors 3 divise aussi x & y, « c-à-d 3 est un facteur commun ».

Si Fermat avait vraiment démontrer son théorème, alors je peux imaginer qu'il savait prouver l'équivalence suivant : « *x^n + y^n = z^n est soluble par entiers non nuls, si et seulement si n & n+1 sont tous les deux des nombres premiers* ».

On note souvent l'opérateur pseudo dérivation par Δ, tel que Δ(f(x))= f(x+1)-f(x), on l'appel aussi la déférence, c'est un opérateur important, car il est analogue à la dérivée, moi je trouve qu'il est important de préciser si cette déférence est à droite ou à gauche, pour cette raisons, je pratique les opérateurs suivants :

La déférence à droite, $\Delta^+\left(f(x)\right)=f(x+1)-f(x)$

La déférence à gauche, $\Delta^-\left(f(x)\right)=f(x)-f(x-1)$

&

La seconde déférence, ou le pas σ par,

$$\sigma\left(f(x)\right)=\Delta^+\left(f(x)\right)-\Delta^-\left(f(x)\right)=f(x+1)+f(x-1)-2f(x)$$

Les fonctions de puissance jouent un rôle important dans la théorie des polynômes, puisque ils font la base canonique de tous les polynômes, pour cette raison je note par :

$$\Delta_n^+(x)=(x+1)^n-x^n$$

$$\Delta_n^-(x)=x^n-(x-1)^n$$

$$\sigma_n(x)=(x+1)^n+(x-1)^n-2x^n$$

Les premiers valeurs du pas,

- $\sigma_1(x)=0$
- $\sigma_2(x)=2$
- $\sigma_3(x)=6x$
- $\sigma_4(x)=12x^2+2$
- $\sigma_5(x)=20x^3+10x$
- $\sigma_6(x)=30x^4+30x^2+2$
- $\sigma_7(x)=42x^5+70x^3+14x$
- $\sigma_8(x)=56x^6+140x^4+56x^2+2$

Là aussi on remarque que $\sigma_2(x)$est toujours divisible par 2, que $\sigma_3(x)$ est toujours divisible par 6, que $\sigma_5(x)$ est toujours divisible par 30, & ..[]..
Et donc,

(24) : pour tout entier n>1, et tout entier x, $\sigma_n(x)\equiv 0$ Modulo(Z(n))

<u>Preuve :</u>
En effet :

$$\sigma_n(x)=\Delta_n^+(x)-\Delta_n^-(x)$$

Et $\Delta_n^+(x)=(x+1)^n-x^n=\left((x+1)^n-(x+1)\right)-\left(x^n-x\right)+1$

De même $\Delta_n^-(x)=x^n-(x-1)^n=\left(x^n-x\right)-\left((x-1)^n-(x-1)\right)+1$

Or d'après (7), on a :

$$\left((x+1)^n-(x+1)\right)\equiv 0\ Modulo(Z_n)$$

Et $\left(x^n-x\right)\equiv 0\ Modulo(Z_n)$

Donc, $\Delta_n^+(x)\equiv 1\ Modulo(Z_n)$

De même, $\Delta_n^-(x) \equiv 1 \; Modulo(Z_n)$

D'où : $\sigma_n(x) \equiv \Delta_n^+(x) - \Delta_n^-(x) \equiv 1-1 \equiv 0 \; Modulo(Z_n)$

C.Q.F.D

Le théorème de Von Staudt-Clausen nous permet d'en déduire que $Z_n b_{n-1} \in \mathbb{Z}$, où b_n dénote les nombre de Bernoulli, en déduit aussi de (24) le résultat suivant :

(25) : $$\forall x \in \mathbb{Z} \text{ alors } b_{n-1}\sigma_n(x) \in \mathbb{Z}$$

En particulier pour x=1, on aura l'opposé d'une séquence des nombres entiers, dite les nombres de Genocchi telle que :

(26) : $$G_n = -b_n \sigma_{n+1}$$

Où $\sigma_n = \sigma_n(1) = 2(2^{n-1} - 1)$ sont des nombres qui ne se terminent jamais avec 8 en base décimale.
Comme les nombres de Bernoulli b_n sont tous nuls pour n impair sauf pour n=1, on déduit la même chose pour les nombres de Genocchi, de plus G_0=0 car vu σ_1=0.

n	0	1	2	3	4	5	6	7	8	9	10
Gn	0	1	−1	0	1	0	−3	0	17	0	−155
Bn	1	−1/2	1/6	0	−1/30	0	1/42	0	−1/30	0	5/66

Nous remarquons que les valeurs non nuls G_n sont impairs, c'est par ce que 2 divise Z_n et σ_n pour tout entier n, mais 4 ne les divises pas.
[]

On peut exprimer les puissances des entiers en terme des pas, tels que :

Cas n=1

$0^1=0$
$1^1=1$
$2^1=1+(1+0)$
$3^1=1+(1+0)+(1+0+0)$
..[]..

Cas n=2

$0^2=0$
$1^2=1$
$2^2=1+(1+2)$
$3^2=1+(1+2)+(1+2+2)$
..[]..

Cas n=3

$0^3=0$
$1^3=1$
$2^3=1+(1+6)$
$3^3=1+(1+6)+(1+6+12)$
$4^3=1+(1+6)+(1+6+12)+(1+6+12+18)$
$5^3=1+(1+6)+(1+6+12)+(1+6+12+18)+(1+6+12+18+24)$
..[]..

(27) : $$\forall \; x \in \mathbb{N}/\{0,1\} \;, \; x^n = 1 + \sum_{j=1}^{x-1}\left(1 + \sum_{t=1}^{j}\sigma_n(t)\right)$$

$0^n=0$, $1^n=1$

Proposition (28) :

Soient p et x deux entiers positive, avec p>2, et $\alpha_{x,p}=\begin{cases}1, \; Si\ p\mid x\\ -1, \; Si\ p\mid x+1\\ 0, \; Sinon\end{cases}$

On a :

Si p est premier alors $\Delta^{+}_{p-1}(x)\equiv\alpha_{x,p}Modulo(p)$

Preuve :

Le choix de p>2, revient à la définition du symbole $\alpha_{x,p}$, si par exemple p=2, on aura pas le troisième cas, pour le quel p ne divise ni x, ni x+1, puisque tout entier est soit pair ou impair.

On a , $\Delta^{+}_{p-1}(x)=(x+1)^{p-1}-x^{p-1}=\left((x+1)^{p-1}-1\right)-\left(x^{p-1}-1\right)$ et on a :

- $(x+1)\wedge x=1$, c'est évident, mais quand même on a, soit d un diviseur commun de x et de x+1, donc $d|x$ et $d|x+1$ donc $d|1$, ce qui fait que d=1.
- D'autre part on applique la forme logique du petit théorème de Fermat, et on a :

$\forall x,p\in\mathbb{N}$, p>2

1ére cas « p divise x »

Si p divise x, alors p est premier avec x+1, et on a :

$$p\ est\ premier\ alors,\begin{cases}(x+1)^{p-1}\equiv 1\ Modulo(p)\\ x^{p-1}\equiv 0\ Modulo\ (p)\end{cases}$$

Donc $\Delta^{+}_{p-1}(x)\equiv 1-0\equiv 1Modulo(p)$.

2éme Cas « p divise x+1 »

Si p divise x+1, alors p est premier avec x, et on a :

$$p\ est\ premier\ alors,\begin{cases}(x+1)^{p-1}\equiv 0\ Modulo(p)\\ x^{p-1}\equiv 1\ Modulo\ (p)\end{cases}$$

Donc $\Delta^{+}_{p-1}(x)\equiv 0-1\equiv -1Modulo(p)$.

3éme Cas « p ne divise ni x, ni x+1 »

Dans ce cas, on a, p ne divise ni x^{p-1}, ni $(x+1)^{p-1}$, donc $x^{p-1}\neq 0$ Modulo (p), et $(x+1)^{p-1}\neq 0$ Modulo (p), il en résulte de la forme logique du petit théorème de Fermat que,

$$p\ est\ premier\ alors,\begin{cases}(x+1)^{p-1}\equiv 1\ Modulo(p)\\ x^{p-1}\equiv 1\ Modulo\ (p)\end{cases}$$

Donc $\Delta^{+}_{p-1}(x)\equiv 1-1\equiv 0Modulo(p)$.

C.Q.F.D

Proposition (29) :

Soient p et x deux entiers positive, avec p > 2, et $\beta_{x,p}=\begin{cases}-1, \; Si\ p\mid x\\ 1, \; Si\ p\mid x-1\\ 0, \; Sinon\end{cases}$

Alors on a :

Si p est premier alors, $\Delta^{-}_{p-1}(x)\equiv\beta_{x,p}Modulo(p)$

Preuve :

On a : $\Delta^{+}f(x-1)=\Delta^{-}f(x)$, en effet : $\Delta^{+}f(x-1)=f(x-1+1)-f(x-1)=\Delta^{-}f(x)$.
On remplace x par x-1 dans la proposition (28), ce qui preuve (29).
C.Q.F.D

Proposition (30) :

$$\text{Soit } \underset{x,p\in\mathbb{N},p\geq 4}{\Gamma_{x,p}} = \begin{cases} 2, & Si\ p \mid x \\ -1, & Si\ p \mid x\pm 1 \\ 0, & Ailleur \end{cases}$$

Si P≥5 est premier alors, $\sigma_{p-1}(x) \equiv \Gamma_{x,p}$ Modulo(p).
Où $\sigma_n(x)$ est le nième pas.

Preuve :
Conséquence immédiate de la proposition (28), et de la proposition (29), puisque $\sigma_{p-1}(x) = \Delta^{+}_{p-1}(x) - \Delta^{-}_{p-1}(x)$
C.Q.F.D

Aspect de Conway

D'après le site d'Eric Weisstein, La partie fractionnaire de b(n) « b(n) est la suite des nombres de Bernoulli », a une représentation décimale périodique, dont la période divise n, les période de {b(n)} pour n=2,4,6,8..[].. sont 1,1,6,1,2,6,1,16,18,2,22..[].. (OEIS A112828).
Cette propriété est décrie par curieuse, et je le trouve vraiment curieuse, même s'elle est très évidente, car ce n'est qu'une conséquence du petit théorème de Fermat et du théorème de Von Staudt & Clausen, et que de plus elle est vraie par rapport a n'importe quelle base, pas seulement la base décimale.
Voici un extrait de ce que Conway a écrit dans son fameux livre « *Famous families of numbers*, page(109) ».

$$B^{12} = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} - \frac{1}{7} - \frac{1}{13} = \frac{-691}{2730} = -.2\dot{5}3113\dot{5}$$

Together with Fermat's Little Theorem this implies that the period of the decimal for B^{2n} has length dividing $2n$, and starts one digit later than the decimal point.

Note that $B^3, B^5, B^7, \ldots$ are all zero, and, although B^2, B^4, B^6 are small, ultimately B^{2n} becomes very large: In fact, it equals

$$\frac{2(2n)!}{(2\pi)^{2n}}\left(1 + \frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \cdots\right).$$

Pour moi la curiosité n'est pas seulement dans ce théorème, ma curiosité est dans une conjecture, dite la conjecture d'Artin, pour Emill Artin, telle que :

(31) : La densité des nombres premiers d'Artin vaut à $C_{Artin} \approx 0.37$.

Les nombres premiers d'Artin sont des nombres premiers qui par rapport à une base donné ils ont une période complète, par exemple par rapport à la base décimale on a :

$$\frac{1}{7} = 0,14285714285714..[]..= 0,\underline{142857}$$

$$\frac{1}{17} = 0,\underline{0588235294117647}$$

$$\frac{1}{19} = 0,\underline{052631578947368421}$$

..[]..

La conjecture veut dire que parmi n nombres premiers successives, il y environ 37% qui ont une période complète.

Note :

La notion des nombres d'Artin est relative, car elle dépendes de la base, par exemple 7 par rapport à la base décimale est un nombre premier d'Artin car son inverse a une période complète, mais il existe d'autre base où son inverse n'a pas une période complète.

Et dans une étude numérique que j'ai fais par ordinateur sur la période des nombres de Bernoulli pour $2 \leq 2n < 67071$, j'ai remarqué la même chose, comme il montre le tableau suivant :

i	x	p1	p2
De b(2) à b(100)	19	38%	38%
b(102) à b(1000)	162	36%	36,20%
b(1002) à b(10000)	1676	37,24%	36,76%
b(10002) à b(20000)	1839	36,78%	36,77%
b(20002) à b(30000)	1790	35,80%	36,45%
b(30002) à b(40000)	1818	36,36%	36,43%
b(40002) à b(50000)	1828	36,56%	36,45%
b(50002) à b(60000)	1788	35,76%	36,37%
b(60002) à b(67070)	1288	36,44%	36,35%

x est le nombre des Bernoulli's dont $\rho(b_{2n}) = 2n$.

p1 est le pourcentage dans l'intervalle i.

p2 est le pourcentage depuis b(2)jusqu'à sup(i).

Et donc suite à la conjecture d'Artin, j'énonce la suivante :

(32) : La densité des nombres de Bernoulli dont la période décimale est complète vaut à $C_{Artin} \approx 0.37$.

Justifions le théorème Conway,

Notation :

On note par l'entier Q≥2 la base du développement décimal, soient n & m deux entiers premiers entre eux, avec n≠0, si n ne divise pas Q ou si une puissance de n ne divise pas la base Q, alors le développement décimal du m/n est infiniment périodique, par exemple Q=10 on a,

$$\frac{1}{56}=0,\underbrace{017}_{\chi=3}\underbrace{857142}_{\rho=6}8571428571..[]..$$

- $\chi(\frac{m}{n})$ est le préfixe.
- $\rho(\frac{m}{n})$ est la période.

Pour le préfixe, il est dû tous simplement au fait que l'entier n contient un diviseur de la base Q, soit d≠1 un diviseur de la base Q, et q le complément de d, « i.e dq=Q », alors on a :

$$\frac{1}{d}=0,q$$

Ainsi $\chi\left(\frac{1}{d}\right)=1$, par exemple pour Q=10 on a,

$$\frac{1}{2}=0,5 \quad \frac{1}{5}=0,2 \quad \& \quad \frac{1}{10}=0,1$$

Mais le préfixe n'est pas toujours égal à 1, est on a,

Si Q est sans facteur carré, $\chi\left(\frac{1}{d^n}\right)=n$, par exemple pour Q=10 on a,

$$\frac{1}{4}=0,25 \quad \frac{1}{8}=0,125 \quad \& \quad \frac{1}{16}=0,0625$$

Note :

Dans la base décimale, on a $\chi\left(\frac{1}{2^n}\right)=\chi\left(\frac{1}{5^n}\right)=\chi\left(\frac{1}{10^n}\right)=n$, pour tout entier n, ceci est vrai seulement si la base Q est sans facteur carré, si Q contient des facteurs carrés comme par exemple Q=16, alors on aura, $\chi\left(\frac{1}{2}\right)=\chi\left(\frac{1}{4}\right)=\chi\left(\frac{1}{8}\right)=\chi\left(\frac{1}{16}\right)=1$, puisque 2,4,8 & 16 sont des diviseurs de Q, dans ce cas particulier on a bien, $\chi\left(\frac{1}{2^n}\right)=\left[\frac{n+3}{4}\right]$ où [ ] désigne la partie entière.

[]

Ceci justifier la proposition suivante :

Proposition (33) :

Soient m et n deux entiers premiers entre eux, avec n≠0, si n est un entier sans facteur carré, alors,

$$\chi\left(\frac{m}{n}\right)=\begin{cases}0, & Si\ (n,Q)=1\\ 1, & Ailleur\end{cases}$$

Exemple pour les nombres de Bernoulli :

Soit Q≥2, et pour tout entier n≥1, on a :

$$\chi(b_{2n}) = \chi\left(\frac{1}{Z_{2n+1}}\right) = \delta$$

Où $\delta \in \{0,1\}$, pour Q=10, on a bien $\delta = 1$, car 2 est toujours un facteur commun entre Z(2n+1) et Q=10.

Proposition (34) :

Soit p un nombre premier qui ne divise pas la base Q≥2, alors on a, ρ(1/p) divise p-1.

C'est un résultat du petit théorème de Fermat, en effet puisque p est premier qui ne divise pas Q, alors p divise $Q^{p-1}-1$, soit N cet entier, on a,

$$N = \frac{Q^{p-1}-1}{p} = \frac{Q^{p-1}}{p} - \frac{1}{p}$$

$$\frac{1}{p} = 0,\underline{a_1 a_2 ..[]..a_\rho}$$

Et donc,

$$\frac{Q^{p-1}}{p} = \underbrace{a_1 a_2 \ ..[].. \ a_\rho a_1 a_2 \ ..[].. \ a_j}_{p-1 \ chiffres} , a_{j+1} a_{j+2} a_{j+3} ..[]..$$

$$j \equiv p-1 \ \ Modulo(\rho)$$

$$j+1 \equiv p \ \ Modulo(\rho)$$

Et pour que la différence soit entière, il faut que les deux parties fractionnaires soient égales, donc

$$1 \equiv p \ \ Modulo(\rho)$$

C.Q.F.D

Proposition (35) :

Soit p un nombre premier qui ne divise pas la base Q≥2, et n un entier non nul, alors on a :

- Si aucune puissance de p n'est égale à (Q-1), alors,

$$\rho\left(\frac{1}{p^n}\right)_{n\in\mathbb{N}^*} = \rho\left(\frac{1}{p}\right)p^{n-1}$$

- Si p^a=Q-1, alors $\rho\left(\frac{1}{p^n}\right)_{n\in\mathbb{N}^*} = \begin{cases} 1, \ si \ n \le a \\ p^{n-a}, \ Ailleurs \end{cases}$

Preuve :

Premier cas, «aucune puissance de p n'est égale à Q-1 »

Soit ρ=ρ(1/p), ce nombre compte les décimaux qui se répètent indéfiniment lorsque on fait la division euclidienne de 1 sur p, mais il compte aussi les résidus qui se répètent indéfiniment, par exemple, 1/11=0.$\underline{09}$ dont les résidus qui se répètent sont 10 & 1, donc d'évidence les résidus de $1/11^n$ seront tous les résidus possibles qui sont congrus à 10 modulo (11) ou à 1 modulo (11), donc il seront au nombre ρp^{n-1}.

Par exemple les résidus de 1/121 sont 10, 100, 32, 78, 54, 56, 76, 34, 98, 12, 120, 111, 21, 89, 43, 67, 65, 45, 87, 23, 109, 1.

Second cas p^a=Q-1

On sait depuis écolier comment calculer les résidus modulo 3 et 9 d'un nombre, par exemple, soit A=25693651, on a, 2+5+6+9+3+6+5+1=37 et 3+7=10 de

même 1+0=1, donc A=1 Modulo(9 ou 3), et on se demande banalement pourquoi seulement 9 et 3 ?
Pour répondre à cette question, je vais changer la base, je prend par exemple Q=626, et on a Q-1=5^4, puis je vais choisir un entier A au hasard en base Q, et pour séparer les décimales qui dépasse un chiffre, je peux utiliser les parenthèses, soit par exemple A= 3829(318)2(417)255(600)3.
Et on a, 3+8+2+9+(318)+2+(417)+2+5+5+(600)+3=2(122)& 2+122=124, donc :

A=4 Modulo(5)
A=24 Modulo(25)
A=124 Modulo(125)
A=124 Modulo(625)

A savoir qu'en base décimale, A= 174295334348891417430111883819999.
Et pour justifier tous ça, alors on a, pour toute base Q≥2,

$$\frac{1}{Q-1}=\sum_{j=1}^{+\infty}Q^{-j}=Q^{-1}+Q^{-2}+Q^{-3}+..[]..=0,\underline{1}$$

Note *: Cette somme est valable pour tout réel Q tel que* $\left|\frac{1}{Q}\right|<1$*, Par exemple,* $0,1=\frac{1}{11}+\frac{1}{121}+\frac{1}{1331}+\frac{1}{14641}+..[]..$

Donc $\rho\left(\frac{1}{Q-1}\right)=1$

Avec 1 comme l'unique résidu qui se répète dans la division Euclidienne de 1/Q-1

Et comme Q-1=p^a alors pour tout n<a on a,

$$\frac{1}{p^n}=\frac{p^{a-n}}{Q-1}=p^{a-n}Q^{-1}+p^{a-n}Q^{-2}+p^{a-n}Q^{-3}+..[]..=0,\underline{(p^{a-n})}$$

Donc $\rho\left(\frac{1}{p^n}\right)=1$

Avec toujours 1 comme l'unique résidus.
Lorsque n dépasse a, cela libère la voie à d'autres résidus autres que 1, ces résidus seront tous congrus à 1 modulo (Q-1), ce qui veut dire qu'ils sont au nombre p^{n-a}.
C.Q.F.D

Exemples :

Q=10,p=3,a=2

1/3=0.$\underline{3}$: ρ=1
1/9=0.$\underline{1}$: ρ=1
1/27=0.$\underline{037}$: ρ=3
1/81=0.$\underline{012345679}$: ρ=9

Q=28,p=3,a=3 *« les chiffres entre parenthèse représente une seule décimale »*

1/3=0.$\underline{9}$: ρ=1
1/9=0.$\underline{3}$: ρ=1
1/27=0.$\underline{1}$: ρ=1
1/3^4=0.$\underline{09(19)}$: ρ=3
1/3^5=0.$\underline{0369(12)(15)(18)(21)(25)}$: ρ=9

1/3^6=0.0123456789(10)(11)(12)(13)(14)(15)(16)(17)(18)(19)(20)(21)(22)(23)(24)(25)(27) : ρ=27

Proposition (36) :

Soit $d=\prod_{\substack{j=1 \\ p_j,premier}}^{n} p_j^{v_j}$, alors on a, $\rho\left(\frac{1}{d}\right)=PPCM\left(\rho\left(\frac{1}{p_j^{v_j}}\right)\right)$.

Preuve :

Cette proposition est un bel exemple du théorème chinois, car d'évidence les résidus de 1/d sont les mêmes que de chaque $1/p_j^{v_j}$, et pour l'éclairer, prenons un exemple,

1/77	10	23	76	67	54	1
1/7	3	2	6	4	5	1
1/11	10	1	10	1	10	1

Cette table représente les résidus de chaque fraction par ordre d'apparition dans la division Euclidienne.
Ainsi le troisième résidu de 1/77 n'est autre que solution du système

$$\begin{cases} x\equiv 6\ Modulo(7) \\ x\equiv 10\ Modulo(11) \end{cases}$$

Dont la plus petite solution qui peut être un résidu est x=76.
Ceci justifier que le nombre des résidus de 1/d vaut au plus petit multiple commun de nombre des résidus de chaque $1/p_j^{v_j}$.
C.Q.F.D

Théorème de Conway (37) :

La partie fractionnaire du nombre b(2n) a une représentation décimale périodique, dont la période divise 2n, où b(n) dénote le nième nombre de Bernoulli.

Preuve :

$\rho(b_{2n})=\rho\left(\frac{1}{Z_{2n+1}}\right)=\underset{p-1|2n}{ppcm}\left(\rho\left(\frac{1}{p}\right)\right)$, or $\rho\left(\frac{1}{p}\right)$divise p-1, donc il divise 2n,

donc $\underset{p-1|2n}{ppcm}\left(\rho\left(\frac{1}{p}\right)\right)$ divise 2n.
C.Q.F.D

Fin

Méhdi Pascal
MehdiPascal38@gmail.com

Références

[1] : Autour des nombres et des polynômes de Bernoulli, Gaëtan Bisson
https://gaati.org/bisson/tea/bernoulli.pdf

[2] : A REVIEW OF THE VON STAUDT CLAUSEN THEOREM, by Timothy Simon Caley.

[3] : Les nombres de Bernoulli, par A. Joyal pour le camp mathématique.

[4] : Eric Weisstein, http://mathworld.wolfram.com/BernoulliNumber.html

[5] : The equation denom(Bn)=n has only one solution, Bernd C. Kellner
2nd April 2005, http://www.bernoulli.org