Fermat revisité

M.Gouy G.Huvent A.Ladureau

10 mars 2003

1 Introduction historique

Le petit théorème de Fermat est un des théorèmes les plus célébres de l'arithmétique[1]. Pour mémoire, on rappelle son énoncé

Théorème 1 (Petit théorème de Fermat) *Soit* p *un entier premier, alors quelque soit l'entier* a, *on a* p *divise* $a^p - a$.

Ce théorème classique peut se démontrer de nombreuses façons différentes[2]. Certaines sont très classiques, d'autres moins. On se propose ici d'en donner quelques unes. Avant cela, il est peut être utile de brosser un rapide portrait de Fermat.

Pierre de Fermat est né en 1601, on a fêté le 400 ième anniversaire de sa naissance en 2001. A cette occasion un timbre poste fut émis. Il meurt en 1665.

Fermat est un mathématicien atypique, il n'a rien d'un génie, il n'est pas précoce et ne travaille pas passionnément, pire, il ne publie pas. Il est conseiller au parlement de Toulouse et n'est qu'un amateur[3] en mathématique. Sa célébrité provient surtout d'une annotation placée en marge d'un exemplaire de *l'arithmétique de Diophante*[4] *:* ≪ Diviser un cube en deux cubes, une puissance quatrième en deux puissances quatrièmes ; ou une puissance quelconque en deux puissances de mêmes dénomination, est impossible ≫ (En termes plus modernes, l'équation $x^n + y^n = z^n$ où $(x, y, z, n) \in (\mathbb{N}^*)^4$ n'a pas de solutions si $n \geq 3$).

Cette affirmation qui porte le nom de Grand théorème de Fermat et dont Fermat affirmait avoir une preuve[5] n'a été démontrée qu'en 1995 par A.Wiles. Quatre cents ans de recherche et le concours des plus grands mathématiciens (Euler, Lagrange, Kummer, Weil entre autres) ont été nécessaires pour en établir une preuve.

Les contributions de Fermat sont cependant très importantes. Pour mémoire citons deux résultats importants :

1) Le petit théorème de Fermat (objet de cette étude), que Fermat cite en 1640 dans une de ses lettres mais ne démontre pas. Les premières preuves sont de Leibniz et Euler.

2) Le théorème des quatre carrés, qui affirme que tout entier est somme de quatre carrés. Lui aussi n'est pas prouvé par Fermat mais par Lagrange.

Il ne faut pourtant pas croire que Fermat s'est toujours contenté d'énoncer des résultats que d'autres se sont chargés de prouver. Il est l'inventeur de la "descente infinie", a développé, avec Pascal, le calcul des probabilités et on lui doit, en optique, le célébre "Principe de Fermat". Il est sans aucun doute l'un des mathématiciens les plus féconds de son époque.

[1] Le Grand théorème de Fermat est tout aussi célébre.
[2] On connaît à ce jour plus de 100 démonstrations différentes du petit théorème de Fermat.
[3] Dans le sens le plus "noble" du terme.
[4] Oeuvres traduites du latin par Bachet de Méziriac, qui est surtout connu pour le théorème de Bachet-Bézout.
[5] Mais la marge semblait, aux dires de Fermat, trop petite pour la contenir.

2 Prérequis : le langage des congruences

2.1 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier au moins égal à 2, on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, ..., n-1\}$$

Lorsque a et b sont deux entiers quelconques, on note

$$a \equiv b \ (n)$$

et on dit que a et b sont congrus modulo n, lorsque $a - b$ est divisible par n.
Ainsi

$$a \equiv b \ (n) \iff n \mid a - b$$

Il existe toujours un **unique** $\alpha \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \equiv \alpha \ (n)$, α est le reste de la division euclidienne de a par n. On écrira que $a = \alpha \mod n$ pour indiquer que α est cet unique entier (en particulier, on a alors $a \equiv \alpha \ (n)$). Par exemple $21 \equiv 11 \ (5)$ et $21 = 1 \mod 5$.
Si a et b sont des entiers, soient α et β congrus à a et b modulo n, alors

$$a \equiv \alpha \ (n) \text{ et } b \equiv \beta \ (n) \Longrightarrow a + b \equiv \alpha + \beta \ (n) \text{ et } ab \equiv \alpha\beta \ (n)$$

Cela permet de définir une addition et une multiplication sur $\mathbb{Z}/n\mathbb{Z}$. Si α et β sont dans $\mathbb{Z}/n\mathbb{Z}$, on définit $\alpha + \beta$ (resp $\alpha\beta$) comme l'unique élément de $\mathbb{Z}/n\mathbb{Z}$ congru à $\alpha + \beta$ (resp $\alpha\beta$) modulo n.

Exemple 2 *Dans* $\mathbb{Z}/5\mathbb{Z}$, *on a la table d'addition suivante*

$a \backslash b$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

et la table de multiplication

$a \backslash b$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

De manière à être cohérent, il faudrait vérifier que l'on a une véritable addition et une véritable multiplication i.e. que l'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de ces deux lois est un anneau. On ne le fera pas car notre objectif est ailleurs.

2.2 Primalité relative

Une notion importante en arithmétique est celle de primalité relative.

Définition 3 *On dit que deux entiers* a *et* n *sont premiers entre eux si leur* pgcd *est égal à* 1.
En d'autres termes si leur seul diviseur commun dans $\mathbb{N}$ *est* 1.

La primalité relative et les congruences se comportent bien entre elles, on a en effet le résultat suivant.

Proposition 4 *Le* pgcd *de* a *et* n *est égal au* pgcd *de* n *et du reste de la division de* a *par* n.
En conséquence, si $a \equiv \alpha\ (n)$, a *est premier avec* n *si et seulement si* α *l'est.*

Enfin on rappelle le résultat suivant, que l'on ne démontre pas ici, car notre propos est ailleurs. Le lecteur intéressé pourra consulter le document de l'Irem de Lille qui lui est consacré.

Théorème 5 (Bachet-Bézout) *Si* a *et* b *sont premiers entre eux , alors il existe* u *et* v *entiers tels que* $au + bv = 1$

Le théorème de Bézout permet ensuite de prouver facilement que

Proposition 6 *Si* a *et* b *sont premiers avec* n, *il en est de même de leur produit* ab.

Lemma 7 (Gauss) *Si* a *et* b *sont premiers entre eux et si* a *divise* bc, *alors* a *divise* c.

On peut maintenant donner différentes preuves du théorème de Fermat.

3 L'approche d'Euler

On définit U_n comme l'ensemble des entiers de $\mathbb{Z}/n\mathbb{Z}$ premier avec n,ainsi

$$k \in U_n \iff \text{pgcd}\,(k, n) = 1$$

On note $\varphi(n)$ le cardinal de U_n, la fonction φ est l'indicateur d'Euler[6].

Exercice 8 *Déterminer* U_n *et* $\varphi(n)$ *pour les premières valeurs de* n. *Que vaut* $\varphi(p)$ *lorsque* p *est premier ?*

L'ensemble U_n est fini, on peut l'écrire $U_n = \left\{a_1, a_2, ..., a_{\varphi(n)}\right\}$.
Soit $a \in U_n$, on définit $b_i = a \times a_i \mod n$, ie b_i est le reste de la division euclidienne de $a \times a_i$ par n.

Exemple 9 *Si* $n = 20$, *les entiers premiers avec* n *sont* $1, 3, 7, 9, 11, 13, 17, 19$ *ainsi* $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$ *et* $\varphi(20) = 8$

Exemple 10 *Pour* $n = 20$ *et* $a = 9$, *on a*

$$a_1, a_2, ..., a_{\varphi(n)} = 1, 3, 7, 9, 11, 13, 17, 19$$

et

$$b_1, ..., b_{\varphi(n)} = 9, 7, 3, 1, 19, 17, 13, 11$$

On constate que l'ensemble des b_i est égal à l'ensemble des a_i. On a simplement effectué une permutation des éléments de U_n.

Proposition 11 *Si* $a \in U_n$ *alors* $\{ax \mod n,\ x \in U_n\} = U_n$

Preuve. *Pour montrer le résultat, il suffit de prouver que*

1. *Les* b_i *sont bien dans* U_n
2. *Ils sont deux à deux distincts*

Les b_i *sont bien dans* U_n, *en effet* a.*et* a_i *sont premiers avec* n *donc d'après la proposition* 6 *le produit* aa_i *aussi. On en déduit (cf proposition 4) que le reste* b_i *de la division de* aa_i *avec* n *l'est aussi.*

Les b_i *sont deux à deux distincts, en effet si, par exemple* $b_1 = b_2$ *alors* n *divise* $a(a_2 - a_1)$ *donc divise* $(a_2 - a_1)$ *d'après le lemme de Gauss. Mais* $-n < a_2 - a_1 < n$ *et est non nul ce qui interdit à* n *de le diviser.*
■

[6] L'entier $\varphi(n)$ est appelé le "totient" de n (ainsi nommé par J.J.Sylvester)

On en déduit donc que $a_1 \times a_2 \times ... \times a_{\varphi(n)} = b_1 \times b_2 \times ... \times b_{\varphi(n)} = a^{\varphi(n)} \times a_1 \times a_2 \times ... \times a_{\varphi(n)}$ (n). En conséquence n divise $\left(a^{\varphi(n)} - 1\right) \times a_1 \times a_2 \times ... \times a_{\varphi(n)}$ et ainsi, puisque n est premier avec $a_1 \times a_2 \times ... \times a_{\varphi(n)}$ (lemme de Gauss), on a démontré le théorème suivant :

Théorème 12 (Euler 1760) *Si* a *et* n *sont premiers entre eux alors* $a^{\varphi(n)} \equiv 1\ (n)$

Un corollaire immédiat est le théorème de Fermat.

Théorème 13 (Fermat 1640) *Si* p *est un nombre premier alors*

$$a^p \equiv a\ (p)$$

4 Fermat via le binôme de Newton

4.1 Le triangle de Pascal modulo n

Soit n un entier, construisons le triangle de Pascal modulo n. On obtient par exemple pour $n = 6$ ou 7

$n = 6$

1									
1	1								ligne 1
1	2	1							ligne 2
1	3	3	1						ligne 3
1	4	0	4	1					⋮
1	5	4	4	5	1				⋮
1	0	3	2	3	0	1			ligne 6
1	1	3	5	5	3	1	1		⋮
1	2	4	2	4	2	4	2	1	⋮

$n = 7$

1									
1	1								ligne 1
1	2	1							ligne 2
1	3	3	1						ligne 3
1	4	6	4	1					⋮
1	5	3	3	5	1				⋮
1	6	1	6	1	6	1			ligne 6
1	0	0	0	0	0	0	1		ligne 7
1	1	0	0	0	0	0	1	1	⋮

On ne peut pas manquer de remarquer cette succession de 0. Quelle est la différence fondamentale entre les nombres 6 et 7 ? La réponse est évidente, 7 est un nombre premier ! Cela incite à prouver le résultat suivant

Proposition 14 *Soit* p *un entier naturel premier et* k *entier tel que* $1 \leq k \leq p-1$ *alors*

$$C_p^k = 0\ (p)$$

Preuve. On sait que $C_p^k = \dfrac{p!}{k!\,(p-k)\,!} = \frac{1}{k!}p\,(p-1)\,...\,(p-k+1)$ donc p divise $k!C_p^k$.Mais p est premier avec $k!$ car premier avec tous les entiers inférieurs à $p-1$. Donc par le lemme de Gauss, p divise C_p^k. ■

4.1.1 Le théorème de Fermat

On en déduit immédiatement que si a et b sont des entiers, alors la formule du binôme de Newton permet d'affirmer que $(a+b)^p \equiv a^p + b^p\ (p)$ pour p premier. Ce résultat n'est pas à proprement dit le théorème de Fermat mais permet facilement de le prouver.

En effet, on a clairement $1^p \equiv 1\ (p)$, puis

$$(1+1)^p = 2^p \equiv 1^p + 1^p \equiv 1 + 1 = 2\ (p)$$

et

$$(1+2)^p = 3^p \equiv 1^p + 2^p \equiv 1 + 2 = 3\ (p)$$

etc[7]...

[7] "*etc*" est une abréviation de "*par récurrence*"

5 Un raffinement : Fermat via le multinôme

La dernière preuve donnée n'est pas des plus satisfaisante, on aimerait écrire que $a^p = (1 + \cdots + 1)^p$ et développer cette puissance. Pour cela il nous faut un outil supplémentaire : la formule du multinôme.

Considérons l'expression $(x_1 + x_2 + \ldots + x_n)^p$ et cherchons à en exprimer le développement. Le coefficient du terme $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$, où $k_1 + k_2 + \ldots + k_n = p$ est obtenu :
En choisissant k_1 fois le terme x_1 parmi les p facteurs
En choisissant k_2 fois le terme x_2 parmi les $p - k_1$ facteurs restants
En choisissant k_3 fois le terme x_3 parmi les $p - k_1 - k_2$ facteurs restants
$\vdots$
En choisissant k_n fois le terme x_n parmi les $p - k_1 - k_2 - \ldots - k_{n-1}$ facteurs restants.
Ainsi le nombre de choix possibles est

$$\begin{aligned} & C_p^{k_1} \times C_{p-k_1}^{k_2} \times C_{p-k_1-k_2}^{k_3} \times \ldots \times C_{p-k_1-k_2-\ldots-k_{n-1}}^{k_n} \\ = & \frac{p!}{k_1!\,(p-k_1)!} \times \frac{(p-k_1)!}{k_2!\,(p-k_1-k_2)!} \times \ldots \times \frac{(p-k_1-k_2-\ldots-k_{n-1})!}{k_n!\,(p-k_1-k_2-\ldots-k_n)!} \\ = & \frac{p!}{k_1!k_2!\ldots k_n!} \text{ car } p - k_1 - k_2 - \ldots - k_n = 0 \end{aligned}$$

On obtient alors la formule du multnôme :

$$(x_1 + x_2 + \ldots + x_n)^p = \sum_{k_1+k_2+\ldots+k_n=p} \frac{p!}{k_1!k_2!\ldots k_n!} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$$

Pour p premier, le coefficient $\dfrac{p!}{k_1!k_2!\ldots k_n!}$ est divisible par p sauf lorsqu'un des k_i est égal à p (et ainsi les autres égaux à 0). On en déduit immédiatement que

$$\text{Si } p \text{ est premier, } (x_1 + x_2 + \ldots + x_n)(x_1 + x_2 + \ldots + x_n)^p \equiv x_1^p + x_2^p + \ldots + x_n^p \ (p)$$

Avec $x_1 = x_2 = \ldots = x_n = 1$, on retrouve le théorème de Fermat.

6 Fermat par les résidus quadratiques

Pour ce sujet (vaste et passionnant) on renvoie le lecteur à [2] et [3]. On va néanmoins donner quelques informations sur la notion de résidu quadratique.

6.1 Le symbole de Legendre

Soit $p \in \mathbb{N}$ un nombre premier, considérons, pour $n \in \mathbb{N}$, l'équation[8] d'inconnue x

$$x^2 = n \ (p)$$

Savoir si cette équation a des solutions, c'est déterminer quand l'entier n est un carré modulo p. On introduit alors le symbole de Legendre.

Définition 15 *Soit $n \in \mathbb{N}$ et p premier, on définit le symbole de Legendre $\left(\frac{n}{p}\right)$ par*

$$\begin{aligned} \left(\frac{n}{p}\right) &= 0 \text{ si } n = 0 \ (p) \\ \left(\frac{n}{p}\right) &= 1 \text{ si } n \neq 0 \ (p) \text{ et } n \text{ est un carré modulo } p \\ \left(\frac{n}{p}\right) &= -1 \text{ si } n \neq 0 \ (p) \text{ et } n \text{ n'est pas un carré modulo } p \end{aligned}$$

[8] Equation que l'on considère, par exemple, lors de la résolution de $ax^2 + bx + c$ modulo p (i.e dans le corps $\mathbb{Z}/p\mathbb{Z}$)

Remarque 16 *Si* $n \neq 0\ (p)$ *alors* $\left(\frac{n}{p}\right)^2 = 1$.

Exemple 17 $\left(\frac{2}{17}\right) = 1$ *car* $6^2 = 36 = 2 + 2 \times 17$

Remarque 18 *Lorsque* p *est premier l'équation* $x^2 = n\ (p)$ *a au plus deux solutions modulo* p.
En effet supposons que $x^2 = n\ (p)$, $y^2 = n\ (p)$ *et* $x \neq y\ (p)$, *alors* $x^2 - y^2 = (x-y)(x+y) = 0\ (p)$.
L'entier p *étant premier avec* $(x-y)$, p *divise* $(x+y)$ *d'où* $y = p - x\ (p)$.
En conclusion si on impose à x *d'être dans* $\{0, 1, ..., p-1\}$ *l'autre solution est* $p - x$.

6.2 Une généralisation du théorème de Wilson

On considère, dans un premier temps un exemple simple. On pose $p = 7$, et on considère les produit xy modulo 7 lorsque x et y sont dans $\mathbb{U}_7 = \{1, 2, 3, 4, 5, 6\}$. On obtient le tableau suivant :

$x \backslash y$	1	2	3	4	5	6
1	1	2	3	**4**	5	6
2	2	**4**	6	1	3	5
3	3	6	2	5	1	**4**
4	**4**	1	5	2	6	3
5	5	3	1	6	**4**	2
6	6	5	**4**	3	2	1

On s'intéresse alors aux solution de l'équation $xy = n\ (7)$ pour les deux cas particuliers $n = 4$ et $n = 3$.

Pour $n = 4$. On constate que pour tout $x \in \mathbb{U}_7$, il existe $y \in \mathbb{U}_7$ tel que $xy = 4\ (7)$.
On a $x = y$ pour deux valeurs de x, à savoir $x_1 = 2$ et $x_2 = p - x_1 = 7 - 2 = 5$. Ces deux entiers sont solutions de l'équation $x^2 = 4$ modulo 7 et cela signifie que 4 est un carré modulo 7, en particulier $\left(\frac{4}{7}\right) = 1$.
Les autres valeurs de x se regroupent en $\frac{(p-1)-2}{2} = \frac{p-3}{2} = \frac{7-3}{2} = 2$ couples : $(1,4)$ et $(3,6)$ dont le produit des éléments vaut toujours 4 modulo 7.
Si l'on considère maintenant le produit $1 \times 2 \times 3 \times 4 \times 5 \times 6 = (p-1)!$. On peut associer les deux racines carrées de 4 et les autres éléments deux par deux pour obtenir

$$(p-1)! = (1 \times 4) \times (6 \times 3) \times (2 \times 5)$$

Le produit des deux racines carrées de 4 est égal à $x_1 \times (p - x_1) \equiv -x_1^2\ (p) \equiv -4\ (7)$. Pour les autres couples, par construction le produit des éléments vaut 4. On obtient donc

$$\begin{aligned}
(p-1)! &= \underbrace{(1 \times 4)}_{=4\ (7)} \times \underbrace{(6 \times 3)}_{=4\ (7)} \times \underbrace{(2 \times 5)}_{=-4\ (7)} \\
&= (4)^{\frac{p-3}{2}} \times (-4) = -n^{\frac{p-1}{2}} \\
&= -4^3\ (7) \\
&= -\left(\frac{4}{7}\right) \times 4^3\ (7)
\end{aligned}$$

Pour $n = 3$, on remarque que si $xy = 3\ (7)$, alors $x \neq y\ (7)$. En effet l'entier 3 n'apparaît pas sur la diagonale et ainsi l'équation $x^2 = 3\ (7)$ n'a pas de solutions. En particulier $\left(\frac{3}{7}\right) = -1$. Les entiers de $\mathbb{U}_7$ se regroupent en $\frac{p-1}{2} = 3$ couples : $(1,3)$, $(2,5)$, $(4,6)$ dont le produit des deux éléments vaut toujours 3.

On a ainsi

$$\begin{aligned}(p-1)! &= \underbrace{(1\times 3)}_{=3\ (7)}\times\underbrace{(2\times 5)}_{=3\ (7)}\times\underbrace{(4\times 6)}_{=3\ (7)}\\ &= n^{\frac{p-1}{2}}\ (p)\\ &= 3^3\ (7)\\ &= -\left(\frac{3}{7}\right)\times 3^3\ (7)\end{aligned}$$

On vient donc, sur un exemple de vérifier le théorème suivant

Théorème 19 (Euler) *Si p est un nombre premier **impair,** et si n n'est pas multiple de p alors*

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

Preuve. *On commence par établir un lemme*

Lemma 20 *Soit p premier et $x\in\mathbb{U}_p=\{1,2,...,p-1\}$ alors il existe un unique $y\in\mathbb{U}_p$ tel que $xy=n\ (p)$.*
Remarque : *Ce résultat se voit également sur le tableau précédent pour lequel $p=7$. Sur chaque ligne apparaît tous les entiers compris entre 1 et 6.*

Preuve. *Puisque p est premier, p et x sont premiers entre eux. Par le théorème de Bézout, il existe u et v tel que $xu+pv=1$. En multipliant par n, on a $xnu+pnv=n$. On prend $y\in\{1,2,...,p-1\}$ tel que $y=nu\ (p)$, y est en fait le reste de la division euclidienne de nu par p. Alors $xy=n\ (p)$, ceci prouve l'existence de y.*
Pour l'unicité, si $xy=xz=n\ (p)$ alors $x(y-z)=0\ (p)\Longrightarrow p$ divise $y-z$. Mais $-p<-(p-1)\leq y-z\leq p-1<p$ donc $y-z=0$.
Ce résultat traduit le fait que $\mathbb{U}_p=(\mathbb{Z}/p\mathbb{Z})^*=\{1,2,...,p-1\}$ est un groupe pour la multiplication. On peut donc résoudre des équations du premier degré. ■

Pour $x\in\mathbb{U}_p$, on note y l'unique élément de $\mathbb{U}_p$ tel que $xy=n\ (p)$. Deux cas se présentent :
Cas 1 : *$x=y$ pour deux valeurs de x notées x_1 et $p-x_1$. Dans ce cas n est résidu quadratique, $\left(\frac{n}{p}\right)=1$ car $x_1^2=n\ (p)$.*
Les $p-3$ autres éléments de $\{1,2,...,p-1\}$ se regroupent en $\frac{p-3}{2}$ paires (x,y) telles que $x\neq y$ et $xy=n\ (p)$. On a alors

$$\begin{aligned}(p-1)! &= n^{\frac{p-3}{2}}\times x_1\times(p-x_1)\ (p)\\ &= n^{\frac{p-3}{2}}\times(-n)\ (p)\\ &= -\left(\frac{n}{p}\right)n^{\frac{p-1}{2}}\ (p)\end{aligned}$$

Cas 2 : *$x\neq y$ pour tout x, n n'est pas résidu quadratique, $\left(\frac{n}{p}\right)=-1$ et les $p-1$ élements de $\{1,2,...,p-1\}$ se regroupent en $\frac{p-1}{2}$ paires (x,y) telles que $x\neq y$ et $xy=n\ (p)$. On a alors*

$$\begin{aligned}(p-1)! &= n^{\frac{p-1}{2}}\ (p)\\ &= -\left(\frac{n}{p}\right)n^{\frac{p-1}{2}}\ (p)\end{aligned}$$

■

En particulier, si l'on prend $n=1$, l'équation

$$x^2=1\ (p)$$

admet deux solutions 1 et -1 donc

$$\left(\frac{1}{p}\right) = 1$$

et le théorème précédent devient le théorème de Wilson[9]

Théorème 21 (Wilson) *Si* p *est premier alors*

$$(p-1)\,! = -1 \ \ (p)$$

La réciproque de ce théorème est également vraie et de démonstration très simple.
En combinant les deux théorèmes précédent, on obtient :

Théorème 22 *Si* p *est premier impair alors*

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

Remarque 23 *Si on élève au carré le résultat précédent, on obtient pour* p *ne divisant pas* n

$$n^{p-1} = 1 \ \ (p)$$

ce résultat est le petit théorème de Fermat.

7 Et le collier se re-ferma(t)

Considérons un collier de p perles formé de perles de n couleurs. Par exemple avec deux couleurs, il existe 6 manières différentes de faire un collier de 4 perles.

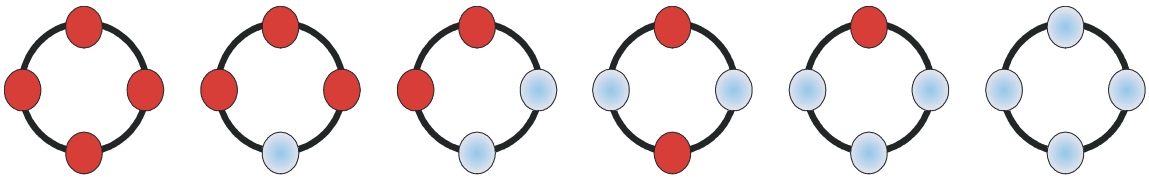


Fig 1.

Les autres configurations possibles sont équivalentes. En effet on peut se ramener à une des configurations de la figure 1. par une rotation du collier.
Par exemple les deux configurations de la figure 2. sont équivalents. On va maintenant dénombrer le nombre de collier **non monochrome**. Pour cela, on part d'un fil et on dispose les p perles. On referme ensuite le fil pour faire un collier. Il y a exactement n^p possibilités d'enfiler les p perles sur le fil. Si on exclue les colliers monochromes, il reste $n^p - n$ possibilités.

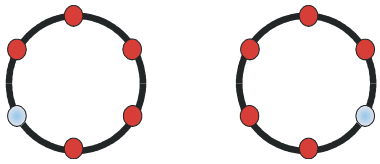


Fig 2.

[9] Wilson John $1741-1793$. Wilson découvre son théorème en 1759 alors qu'il est étudiant mais ne le publie pas et n'en donne pas de démonstration. La première publication, toujours sans démonstration est due à Waring, il est ensuite démontré par Lagrange. Cependant ce résultat était déjà connu de Leibniz.

Le problème provient du fait que des enfilages différents peuvent produire le même collier. Par exemple le second collier de la figure 1, provient des enfilages suivants (cf figure 3. où l'on peut faire quatre coupure, la flèche indiquant le sens d'enfilage des perles). On constate que ce collier provient de 4 fils différents.

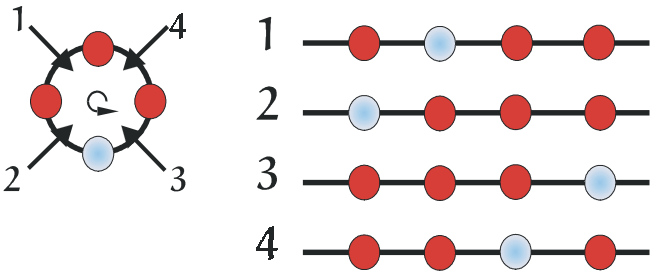
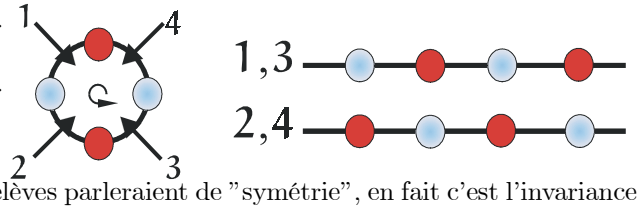


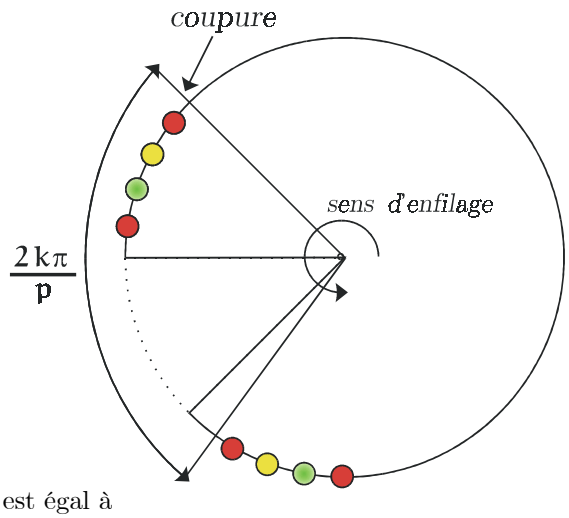
Fig 3.

Il y a clairement p points de coupures pour le collier donc au plus p fils différents donnant le même collier. **Au plus**, car dans l'exemple 1, le $4-$ième collier provient de deux fils.



Quelle est la particularité de ce dernier collier ? Nos élèves parleraient de "symétrie", en fait c'est l'invariance par une rotation non triviale qui est fondamentale (pourvu que l'on dispose les perles aux sommets d'un polygone régulier). Pour se convaincre, essayons de construire un collier à 30 perles (de deux couleurs différentes) qui soit issu de moins de 30 fils différents. C'est assez simple, puisque $30 = 5 \times 3 \times 2$,on dispose 6 perles et on répète ce motifs 4 fois de plus.
On comprends bien que si p est premier, chaque collier provient exactement de p fils distincts.

En effet, supposons le contraire et disposons les perles aux sommets d'un polygone régulier à p côtés de centre O. Par hypothèse, il existe deux coupures distinctes donnant le même enfilage. Si l'on place ces coupures au milieu des côtés du polygône, les deux coupures sont séparées d'un angle de $\frac{2k\pi}{p}$. La rotation d'angle $\frac{2k\pi}{p}$ et de centre O laisse alors invariant le collier. Puisque p est premier avec k, par Bézout, on peut trouver u et v tels que $ku + pv = 1$.Mais alors en composant u fois la rotation initiale, on obtient une rotation d'angle $\frac{2\pi}{p} \times (1 - pv) \equiv \frac{2\pi}{p}\ (2\pi)$. Dans ce cas, toutes les perles ont même couleur (car la rotation d'angle $\frac{2\pi}{p}$remplace une perle par sa voisine).



En conclusion, si p est premier, le nombre de colliers est égal à

$$\boxed{\frac{n^p - n}{p}}$$

qui est **un entier**, d'où le théorème de Fermat.

Remarque : De manière générale, le problème de la détermination du nombre de collier de p perles ayant n couleurs possibles a été résolu par P.A. MacMahon en 1892 (cf [1], p.150).
La réponse est

$$\frac{1}{p}\sum_{d|p} n^{\frac{p}{d}}\varphi(d)$$

où la somme porte sur les diviseurs de p.

Lorsque p est premier, on obtient

$$\frac{1}{p}\left(n^p\varphi(1)+n\varphi(p)\right)=\frac{1}{p}\left(n^p+n(p-1)\right)=n+\frac{n^p-n}{p}$$

et l'on retrouve le théorème de Fermat.

8 A propos de la réciproque du théorème de Fermat

On peut se poser la question de la réciproque du théorème de Fermat.
Soit p un entier tel que pour tout a entier, on a p divise a^p-a. L'entier p est-il premier ?
On peut être tenté de formuler une autre réciproque plus restrictive .
Soit p un entier tel que pour tout a entier premier avec p, on a p divise $a^{p-1}-1$. L'entier p est-il premier ?
Montrons que la réponse à la seconde question est oui si l'on impose certaines conditions à a, mais non dans le cas général.

8.1 Une "réciproque" du théorème de Fermat

Théorème 24 *Pour qu'un entier $p\geq 2$ soit premier, il faut et il suffit que*

$$\forall a\in\{1,2,\cdots,p-1\},\ a^{p-1}\equiv 1\ (p)$$

Preuve. *D'après Fermat, la condition est nécessaire. On montre qu'elle est suffisante. Soit p vérifiant cette condition. On utilise alors le lemme suivant.*

Lemma 25 *Soit $(a,p)\in\mathbb{Z}^2$ alors a et p sont premiers entre eux si et seulement s'il existe $b\in\mathbb{Z}$ tel que $ab\equiv 1\ (p)$.*
En d'autres termes, a et p sont premiers entre eux si et seulement si a est inversible modulo p.
(On pourra comparer ce lemme et le lemme 20).

Preuve de lemme. *On travaille par équivalence*

$$\begin{aligned} a \text{ et } p \text{ premiers entre eux} &\iff \exists(u,v)\in\mathbb{Z}^2,\ au+pv=1\\ &\iff \exists b\in\mathbb{Z},\ ab\equiv 1\ (p)\end{aligned}$$

■

On revient alors à la démonstration du théorème. D'après le lemme, l'entier p est premier avec $1,2,\cdots,p-1$, il est donc premier (il n'a pas de diviseur strict). ■

On va maintenant examiner la réciproque du théorème de Fermat.

8.2 Nombres de Carmichael

Considérons l'entier $p=561=3\times 11\times 17$. D'après Fermat, on a, pour a entier premier avec 561

$$a^2 \equiv 1\ (3) \tag{1}$$
$$a^{10} \equiv 1\ (11) \tag{2}$$
$$a^{16} \equiv 1\ (17) \tag{3}$$

En effet a est alors premier avec $3,11$ et 17. On utilise ensuite la propriété suivante

Proposition 26 *Soit* m *et* n *deux entiers premiers entre eux. Soit* a *un entier tel que*

$$a \equiv b \ (m) \ \text{et} \ a \equiv b \ (n)$$

alors

$$a \equiv b \ (mn)$$

Preuve. *En effet* m *divise* $a - b$. *Il existe donc* c *tel que* $a - b = mc$. *Puisque* n *est premier avec* m, *par le théorème de Gauss, on en déduit que* n *divise* c. *En définitive* $m \times n$ *divise* $a - b$. ■

D'après les égalités (1), (2) et (3) on a

$$a^{2\times 10\times 16} = a^{320} \equiv 1 \ (561)$$

On remarque alors que $2 = 3 - 1$ divise 560, $10 = 11 - 1$ divise 560 et enfin $16 = 17 - 1$ divise 560. On peut ainsi affirmer que

$$\text{Pour tout entier } a \text{ premier avec } 561, \text{ on a } a^{560} \equiv 1 \ (561)$$

Ce qui prouve que la réciproque du théorème de Fermat est fausse. L'entier 561 est dit un nombre de Carmichael.

Définition 27 *L'entier* n *est dit de Carmichael*[10] *si* n *est non premier et si pour tout* a *premier avec* n, *on a*

$$a^{n-1} \equiv 1 \ (n)$$

Remarque 28 *On pourra consulter avec profit le document où l'on expose un critère de primalité probabiliste pour lequel les nombres de Carmichael s'avèrent génants.*

En examinant le cas de l'entier 561, on constate que la proposition suivante est vraie.

Proposition 29 (Critère de Korselt (1899)) *Soit* n *un entier non premier, sans facteur carré*[11] *et tel que pour tout diviseur* p *premier de* n *on a* $p - 1$ *divise* $n - 1$, *alors* n *est un entier de Carmichael.*

Remarque 30 *En fait, on peut montrer que l'on obtient ainsi tous les entiers de Carmichael cf [4].*

On signale qu'un tel entier est nécessairement impair (car s'il admet deux facteurs premiers, l'un deux, noté p est impair. Puisque $p - 1$ divise $n - 1$, on en déduit que $n - 1$ est pair)

8.3 Quelques résultats sur ces entiers

Un entier de Carmichael est nécessairement impair. En effet s'il admet deux facteurs premiers, l'un des deux, noté p est impair. Puisque $p - 1$ divise $n - 1$, on en déduit que $n - 1$ est pair.
Les entiers de Carmichael ont nécessairement au moins trois facteurs premiers distincts. En effet si $n = pq$ avec $p < q$, on sait que $q - 1$ divise $pq - 1 = p(q - 1) + (p - 1)$ donc $q - 1$ divise $p - 1$, ce qui est absurde ($p < q$).

On peut obtenir des entiers de Carmichael en les cherchant sous la forme $(2a + 1)(10a + 1)(16a + 1)$, il faut alors que les trois facteurs soient des nombres premiers. C'est le cas si $a = 1$ (qui donne 561 et explique pourquoi on les a cherchés sous cette forme) mais aussi si $a = 6$ ($n = 76921$), ou $a = 15$ ($n = 1128121$). Une autre famille intéressante est de la forme $(6a + 1)(12a + 1)(18a + 1)$ qui donne avec $a = 1$ et $a = 6$ les entiers $n = 1729$ et $n = 294409$.
La liste des premiers nombres de Carmichael est la suivante : $561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841$
Les nombres de Carmichael sont assez rares, mais on sait depuis 1994 qu'il en existe une infinité. Plus précisément on a le théorème suivant.

Théorème 31 (Alford, Granville, Pomerance) *Pour* x *assez grand, il existe au moins* $x^{\frac{2}{7}}$ *nombres de Carmichael inférieurs à* x.

[10] CARMICHAEL Robert Daniel (1879-1967) Physicien puis Mathématicien Américain.

[11] n peut s'écrire $n = p_1 p_2 \cdots p_k$ où les p_i sont premiers deux à deux distincts.

Références

[1] *Mathématiques Concrètes-Fondations pour l'informatique,*R.Graham, D.Knuth, O.Patashnik, International Thomson Publishing France, Paris, 1998

[2] *An Introduction to the Theory of Numbers*, Fifth edition, G.H.Hardy, E.M.WRIGHT. Oxford Science Publications (Traduction fracnçaise à paraître chez Springer Verlag)

[3] *Théorie des nombres*, D.Duverney, Dunod

[4] *Cours de Cryptographie*, G.Zemor, Cassini

[5] *Les nombres premiers*, M.Gouy, G.Huvent, A.Ladureau, Publication de l'Irem de Lille