Des Carrés dans les Nombres Pointés

Lycée Saint Joseph de Bressuire (79)
Bilan de l'année scolaire 2003/2004

Et si $\dot{6} \times \dot{5} = \dot{2}$?

Et si $\left(\dot{4}\right)^2 = \dot{\overline{-1}}$?

Des Carrés Modulo *p*

Définitions:

Modulo 7, on note $\dot{2}$ l'ensemble

$\dot{2} = \{2;9;16;23;\ldots -5;-12;\ldots\}$

Plus concrètement:
On considère un déplacement dans le sens direct sur un cercle d'un quart de tour.
Au bout de 4 déplacements, le tour du cercle est fait, de même au bout de 8 déplacements on est

On note F_7 l'ensemble $F_7 = \left\{\dot{0}; \dot{1}; \dot{2}; \dot{3}; \dot{4}; \dot{5}; \dot{6}\right\}$;

$\dot{x} = \{x;\ x+7;\ x+2\times 7;\ x+3\times 7;...x-7;\ x-2\times 7;...\}$

Modulo *p*, on note $\dot{2}$ l'ensemble

$\dot{2} = \{2;\ 2+p;\ 2+2p;\ 2+3p;...2-p;\ 2-2p;...\}$

On note F_p l'ensemble $F_p = \left\{\dot{0}; \dot{1}; \dot{2}; \dot{3};...;\ \dot{\overline{p-1}}\right\}$

$\dot{x} = \{x;\ x+p;\ x+2p;\ x+3p;...x-p;\ x-2p;...\}$

L'addition se définit dans F_p par $\dot{x}+\dot{y} = \dot{\overline{x+y}}$,

par exemple dans F_7 on a $\dot{6}+\dot{3} = \dot{9} = \dot{2}$.

De même la multiplication se définit par

$\dot{x}\times\dot{y} = \dot{\overline{x\times y}}$

par exemple dans F_7 : $\dot{6}\times\dot{5} = \dot{30} = \dot{2}$

revenu au point de départ; les positions possibles sont notées $\dot{0}; \dot{1}; \dot{2}; \dot{3}$: on note

$F_4 = \left\{\dot{0}; \dot{1}; \dot{2}; \dot{3}\right\}$

Se déplacer d'un quart de tour, ou de 5 quarts de tour ou de 9 quart de tour revient au même: on pourrait noter ainsi dans F_4 : $\dot{1} = \dot{5} = \dot{9}$.

Avec des déplacements d'un sixième de tour, on aurait $F_6 = \left\{\dot{0}; \dot{1}; \dot{2}; \dot{3}; \dot{4}; \dot{5}\right\}$ et on pourrait écrire

$\dot{1} = \dot{7} = \dot{13}$; de même $\dot{2} = \dot{8} = \dot{14}$.

De même pour les mesures en radians des angles orientés, on retrouve par exemple que $\pi/2$ et $-3\pi/2$ mesurent le même angle modulo 2π. On note $\dot{\overline{\pi/2}} = \dot{\overline{-3\pi/2}}$ modulo 2π

Dans les tables de multiplication,
le zéro apparaît dans la table,
même si les deux nombres multipliés ne sont pas nuls par exemple dans F_8 : $\dot{2}\times\dot{4} = \dot{0}$. On avait pensé qu'il ne fallait travailler qu'avec les nombres impairs, mais à cause des calculs dans F_9 où on a trouvé que $\dot{3}\times\dot{3} = \dot{0}$,
seuls les nombres premiers ont été utilisés comme "modulo".

Pratiquement:

Par exemple dans F_7 , $\dot{6}\times\dot{5} = \dot{30} = \dot{2}$ en faisant la division

30	7
2	4

Premiers calculs:
tables d'addition et de multiplication

Théorème de l'unicité:

Dans $F_p = \left\{\dot{0}; \dot{1}; \dot{2}; \dot{3};...;\ \dot{\overline{p-1}}\right\}$ avec *p* premier, dans la table de multiplication, chaque nombre pointé sauf $\dot{0}$ est obtenu une fois et une seule dans chaque ligne et chaque colonne.

Démonstration: voir annexe 1

On admet le théorème de Gauss:
Si un nombre *a* divise le produit *bc*
et si *a* et *b* n'ont pas de diviseur commun,
alors *a* divise *c*.

4 propriétés ont été trouvées et démontrées.

Théorème de la première symétrie: Dans F_p, on a $\left(\dot{x}\right)^2 = \left(\dot{\overline{p-x}}\right)^2$

Démonstration: voir annexe 2

Théorème du nombre de carrés non nuls:

Le nombres de carrés non nuls différents obtenus dans F_p est donné par la formule $c_p^* = \frac{p-1}{2}$.

Démonstration: voir annexe 3

Théorème de la somme des carrés:

Dans F_p, on a $\left(\dot{1}\right)^2 + \left(\dot{2}\right)^2 + \left(\dot{3}\right)^2 + \ldots + \left(\overline{\dot{p-1}}\right)^2 = \dot{0}$ pour *p* premier supérieur à 3.

Démonstration: voir annexe 4

Théorème des puissances: Dans F_p, pour tout $\dot{x}$, $\left(\dot{x}\right)^{p-1} = \dot{1}$.

Démonstration: voir annexe 5

D'autres observations ont permis de faire des propositions que nous n'avons pu démontrer à ce jour**:**

Conjecture de $\overline{\dot{-1}}$ carré: Pour *p* premier avec $p = 4n+1$, dans F_p, $\overline{\dot{-1}}$ est obtenu comme carré

Voir annexe 6

Conjecture de la deuxième symétrie:

Pour *p* premier avec $p = 4n+1$, dans F_p : si $\dot{y}$ est un carré, alors $\overline{\dot{p-y}}$ est un carré

Ce résultat a été qualifié de "belle conjecture" par le chercheur.
Voir annexe 7

Comme **prolongements** il est sans doute possible de:

- démontrer les deux propositions précédentes,
- conjecturer la condition sur *p* pour que $\dot{a}$ soit un carré dans F_p,
- conjecturer les carrés obtenus dans F_p.

Annexe 1: Unicité

Lorsque le module p est un nombre premier.

$\mathbb{F}7$

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{1}$	$\dot{3}$	$\dot{5}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{6}$	$\dot{2}$	$\dot{5}$	$\dot{1}$	$\dot{4}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{1}$	$\dot{5}$	$\dot{2}$	$\dot{6}$	$\dot{3}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{3}$	$\dot{1}$	$\dot{6}$	$\dot{4}$	$\dot{2}$
$\dot{6}$	$\dot{0}$	$\dot{6}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

pour tout $x \neq \dot{0}$ et $p > x > 0$

Supposons que $x\dot{a} = x\dot{b}$

par définition $xa - xb = kp$ $(k \neq 0)$

$x(a-b) = kp$

p, divise alors $x(a-b)$

or d'après le théorème de Gauss, p ne peut pas diviser x car $p > x$

donc p divise $(a-b)$

d'où $(a-b)$ est multiple de p

donc $(a \dot{-} b) = \dot{0}$

alors $\dot{a} = \dot{b}$

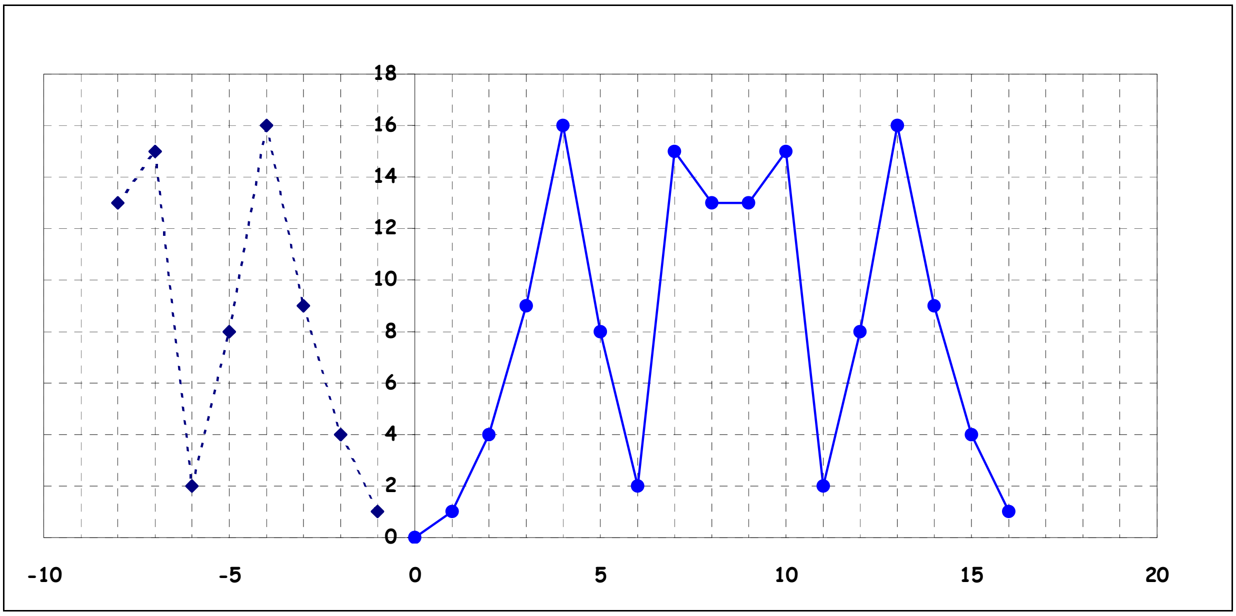
Annexe 2: 1ère symétrie

Dans $F_p = \left\{\dot{0}; \dot{1}; \dot{2}; \dot{3}; \ldots; \dot{\overline{p-1}}\right\}$

$\left(\dot{x}\right)^2 = \left(-\dot{x}\right)^2$ en utilisant que $\left(-\dot{x}\right)^2 = [\left(-\dot{1}\right) \times \left(\dot{x}\right)]^2 = \left(-\dot{1}\right)^2 \times \left(\dot{x}\right)^2 = \left(\dot{x}\right)^2$

$\dot{\overline{x-p}} = \dot{x} - \dot{p} = \dot{x}$ donc $\left(\dot{x}\right)^2 = \left(\dot{\overline{p-x}}\right)^2$

Cette démonstration se voit sur la représentation de $(\overset{*}{x}, \overset{*}{x}{}^2)$ avec $p = 31$



Annexe 3: nombre de carrés

Ce résultat a été trouvé à partir de tableaux de ce type

p = 13

$\dot{x}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{10}$	$\dot{11}$	$\dot{12}$	**Nombre de carrés**
$\dot{x}^2$	$\dot{1}$	$\dot{4}$	$\dot{9}$	$\dot{3}$	$\dot{12}$	$\dot{10}$	$\dot{10}$	$\dot{12}$	$\dot{3}$	$\dot{9}$	$\dot{4}$	$\dot{1}$	**6**

1) Dans $F_p = \left\{\dot{0}; \dot{1}; \dot{2}; \dot{3}; \ldots; \dot{\overline{p-1}}\right\}$ avec p premier, il y a au maximum p carrés différents

2) Comme $\left(\dot{x}\right)^2 = \left(\dot{\overline{p-x}}\right)^2$ il y a au plus $\dfrac{p-1}{2}$ carrés, p étant impair

3) On a $\left(\dot{x}\right)^2 = \left(\dot{y}\right)^2$ lorsque $\left(\dot{x}\right)^2 - \left(\dot{y}\right)^2 = 0$ c'est à dire lorsque $\left(\dot{x} - \dot{y}\right) \times \left(\dot{x} + \dot{y}\right) = 0$ ce qui est vérifié seulement lorsque $\left(\dot{x} - \dot{y}\right) = 0$ ou $\left(\dot{x} + \dot{y}\right) = 0$ ce qui donne $\left(\dot{x}\right) = \left(\dot{y}\right)$ ou $\left(\dot{x}\right) = -\left(\dot{y}\right)$ ce qui est impossible en prenant $0 \le x < y \le \dfrac{p-1}{2}$ car $-\left(\dot{y}\right) = \left(\dot{\overline{-y}}\right) = \left(\dot{\overline{p-y}}\right)$ et $p - y \ge \dfrac{p-1}{2}$

4) Il existe donc exactement $\dfrac{p-1}{2}$ carrés.

Annexe 4: somme des carrés

La propriété a été conjecturée à partir de tables des carrés comme celles-ci:

p = 11

$\dot{x}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{10}$	**Somme**
$\dot{x}^2$	$\dot{1}$	$\dot{4}$	$\dot{9}$	$\dot{5}$	$\dot{3}$	$\dot{3}$	$\dot{5}$	$\dot{9}$	$\dot{4}$	$\dot{1}$	$\overset{*}{44} = \overset{*}{0}$

p = 13

$\dot{x}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{10}$	$\dot{11}$	$\dot{12}$	**Somme**
$\dot{x}^2$	$\dot{1}$	$\dot{4}$	$\dot{9}$	$\dot{3}$	$\dot{12}$	$\dot{10}$	$\dot{10}$	$\dot{12}$	$\dot{3}$	$\dot{9}$	$\dot{4}$	$\dot{1}$	$\overset{*}{78} = \overset{*}{0}$

p = 17

$\dot{x}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{10}$	$\dot{11}$	$\dot{12}$	$\dot{13}$	$\dot{14}$	$\dot{15}$	$\dot{16}$	**Somme**
$\dot{x}^2$	$\dot{1}$	$\dot{4}$	$\dot{9}$	$\dot{16}$	$\dot{8}$	$\dot{2}$	$\dot{15}$	$\dot{13}$	$\dot{13}$	$\dot{15}$	$\dot{2}$	$\dot{8}$	$\dot{16}$	$\dot{9}$	$\dot{4}$	$\dot{1}$	$\overset{*}{136} = \overset{*}{0}$

1) On a $(\dot{x})^2 = \dot{x} \times \dot{x} = \overset{*}{\overline{x \times x}} = (\dot{x^2})$ et $\dot{x} + \dot{y} = \dot{\overline{x+y}}$

2) De même $\left(\dot{1}\right)^2 + \left(\dot{2}\right)^2 + \left(\dot{3}\right)^2 + \ldots + \left(\dot{\overline{p-1}}\right)^2 = \overset{*}{\overline{1^2 + 2^2 + \ldots + (p-1)^2}}$

3) De plus par récurrence, on démontre que $1^2 + 2^2 + \ldots + (p-1)^2 = \dfrac{(p-1)p(2p-1)}{6}$

4) (p-1) est pair donc multiple de 2; si (p-*1*) est multiple de 3 alors $(p-1)p(2p+1) = 6K$,
sinon p ne peut être que de la forme 3k+2 , dans ce cas 2p-1 est de la forme 6k+3 donc multiple de 3, d'où $(p-1)p(2p+1) = 6pK$

5) donc $\left(\dot{1}\right)^2 + \left(\dot{2}\right)^2 + \left(\dot{3}\right)^2 + \ldots + \left(\dot{\overline{p-1}}\right)^2 = \overset{*}{\overline{1^2 + 2^2 + \ldots + (p-1)^2}} = \overset{*}{\overline{\dfrac{p(p+1)(2p+1)}{6}}} = \overset{*}{\overline{p \times K}} = \overset{*}{0}$

Annexe 5: puissance (p-1)ème

Pour les nombres premiers $\dot{x}^{p-1} = \dot{1}$ I

p = 13

$\dot{x}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{10}$	$\dot{11}$	$\dot{12}$
$\dot{x}^2$	$\dot{1}$	$\dot{4}$	$\dot{9}$	$\dot{3}$	$\dot{12}$	$\dot{10}$	$\dot{10}$	$\dot{12}$	$\dot{3}$	$\dot{9}$	$\dot{4}$	$\dot{1}$
$\dot{x}^3$	$\dot{1}$	$\dot{8}$	$\dot{1}$	$\dot{12}$	$\dot{8}$	$\dot{8}$	$\dot{5}$	$\dot{5}$	$\dot{1}$	$\dot{12}$	$\dot{5}$	$\dot{12}$
$\dot{x}^6$	$\dot{1}$	$\dot{12}$	$\dot{1}$	$\dot{1}$	$\dot{12}$	$\dot{12}$	$\dot{12}$	$\dot{12}$	$\dot{1}$	$\dot{1}$	$\dot{12}$	$\dot{1}$
$\dot{x}^{12}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$

ligne 1 : $\dot{1} \times \dot{2} \times \ldots \times \dot{\overline{p-1}} = P_1$

ligne x : $(\dot{1} \times \dot{x}) \times (\dot{2} \times \dot{x}) \times \ldots \times (\dot{x} \times (\dot{p-1}))$
$= P_x$

p = 17

$\dot{x}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{10}$	$\dot{11}$	$\dot{12}$	$\dot{13}$	$\dot{14}$	$\dot{15}$	$\dot{16}$
$\dot{x}^2$	$\dot{1}$	$\dot{4}$	$\dot{9}$	$\dot{16}$	$\dot{8}$	$\dot{2}$	$\dot{15}$	$\dot{13}$	$\dot{13}$	$\dot{15}$	$\dot{2}$	$\dot{8}$	$\dot{16}$	$\dot{9}$	$\dot{4}$	$\dot{1}$
$\dot{x}^4$	$\dot{1}$	$\dot{16}$	$\dot{13}$	$\dot{1}$	$\dot{13}$	$\dot{4}$	$\dot{4}$	$\dot{16}$	.	.	.	.	.	.	.	.
$\dot{x}^8$	$\dot{1}$	$\dot{1}$	$\dot{16}$	$\dot{1}$	$\dot{16}$	$\dot{16}$	$\dot{16}$	$\dot{1}$	.	.	.	.	.	.	.	.
$\dot{x}^{16}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	$\dot{1}$	.	.	.	.	.	.	.	.

Donc $P_x = (\dot{1} \times \dot{x}) \times (\dot{2} \times \dot{x}) \times \ldots \times (\dot{x} \times (\dot{p-1}))$

$= (\dot{x})^{p-1} \times \dot{1} \times \dot{2} \times \ldots \times (\dot{p-1})$

Or dans la ligne x on retrouve chaque nombre pointé 1 fois et une seule.

Donc $P_x = \dot{1} \times \dot{2} \times \ldots \times \dot{\overline{p-1}}$

alors $P_x = (\dot{x})^{p-1} \times \dot{1} \times \dot{2} \times \ldots \times (\dot{p-1}) = \dot{1} \times \dot{2} \times \ldots \times (\dot{p-1})$

On peut donc simplifier $(\dot{x})^{p-1} = \dot{1}$

Annexe 6: $\overset{*}{\overline{-1}}$ **carré**

Des listes des carrés ont été établies:

p	5	7	11	13	17	19	23	29	31	37	41
	1	1	1	1	1	1	1	1	1	1	1
	4	2	3	3	2	4	2	4	2	3	2
		4	4	4	4	5	3	5	4	4	4
			5	9	8	6	4	6	5	7	5
			9	10	9	7	6	7	7	9	8
				12	13	9	8	9	8	10	9
					15	11	9	13	9	11	10
					16	16	12	16	10	12	16
						17	13	20	14	16	18

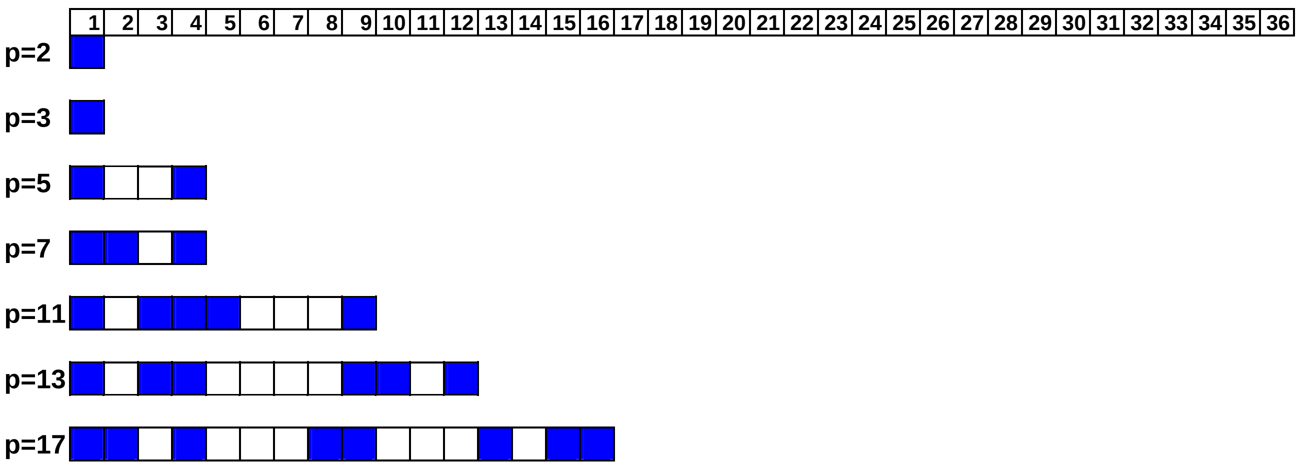
16	22	16	21	20
18	23	18	25	21
	24	19	26	23
	25	20	27	25
	28	25	28	31
		28	30	32
			33	33
			34	36
			36	37
				39
				40

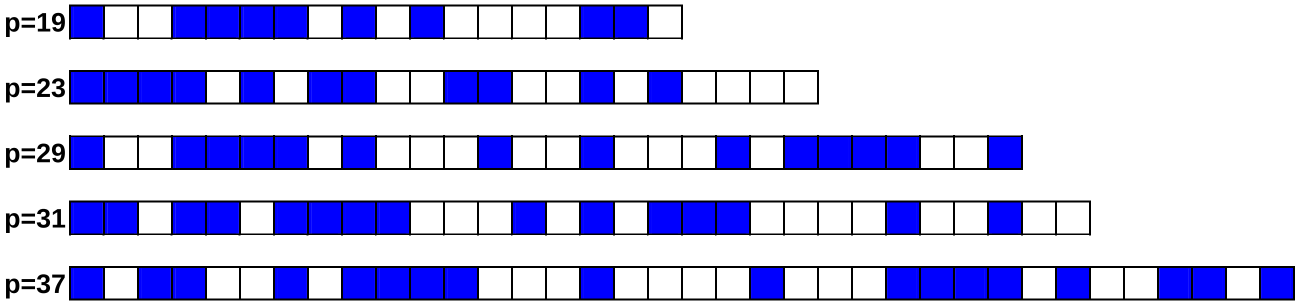
La conjecture "lorsque p est de la forme $4n+1$, $\overset{*}{\overline{-1}} = \overset{*}{\overline{p-1}}$ est un carré" a été établie.
Mais le groupe n'a pas démontré ce résultat

Annexe 7: 2ème symétrie
Des listes de carrés ont été calculées

p	**5**	**7**	**11**	**13**	**17**	**19**	**23**
x	**x^2**						
1	1	1	1	1	1	1	1
2	4	4	4	4	4	4	4
3	4	2	9	9	9	9	9
4	1	2	5	3	16	16	16
5		4	3	12	8	6	2
6		1	3	10	2	17	13
7			5	10	15	11	3
8			9	12	13	7	18
9			4	3	13	5	12
10			1	9	15	5	8
11				4	2	7	6
12				1	8	11	6
13					16	17	8
14					9	6	12
15					4	16	18
16					1	9	3
17						4	13
18						1	2
19							16
20							9
21							4
22							1

puis ordonnées et représentées





Le groupe a conjecturé le résultat suivant,

" Pour p premier avec $p = 4n+1$, dans F_p : si $\dot{y}$ est un carré, alors $\overline{\dot{p-y}}$ est un carré"
mais il n'a pu le démontrer.

En guise de conclusion:

L'année en question a été la première année de fonctionnement d'un club MATh.en.JEANS dans le Lycée Saint Joseph de Bressuire:
d'une part nous avions tout à apprendre
- découverte, par le chercheur, du principe, ainsi que des programmes et savoir-faire des élèves,
- pour les élèves, prise en main d'une autre pratique avec de nouvelles étapes,
- pour les enseignants, heureusement que nous étions trois pour répartir un peu les tâches;

d'autre part
- le chercheur n'a pu, pour des raisons de santé, nous accompagner jusqu'au bout,
- nous n'avons pu conduire les élèves jusqu'au terme du parcours (compte-rendu écrit)

malgré tout
- ce compte-rendu fait par les enseignants essaie de rendre compte des résultats obtenus,
- ce sont bien les élèves qui ont faits les observations et proposé les conjectures,
- ce sont évidemment les élèves de terminale qui ont été les plus moteurs pour les démonstrations,
- la dernière conjecture a été trouvée par un élève de seconde grâce à une nouvelle représentation.

A propos de cette dernière conjecture voici la réponse du chercheur

Un élève, après avoir représenté les carrés obtenus, a remarqué la symétrie des carrés dans certains cas:
> "Pour p premier et p=4n+1, dans Z/pZ : si y est un carré, alors(p-y) est aussi un carré"
> La démonstration est-elle simple ? A jeudi.

je réponds à ta question. Il n'y a pas de démonstration simple.
Et il faut AU MINIMUN le petit théorème de Fermat.
C'est déjà très bien que l'élève ait remarqué cela !
Son assertion est équivalente au fait que -1 est un carré modulo p.
Si l'on utilise le critère
"a est un carré modulo p si et seulement si a^{(p-1)/2} est congru à 1modulo p"
alors c'est clair car (-1)^{(p-1)/2}=(-1)^{2n}=1.
Encore faut-il démontrer le critère...
Cela revient à factoriser a^{p-1}-1 =[a^{(p-1)/2}-1][a^{(p-1)/2}+1]
d'appliquer le petit théorème de Fermat
et de voir que les résidus quadratiques sont racines du premier facteur mais pas du second.
Ca n'est pas du tout évident.
Je réfléchis à une alternative, mais je ne suis pas très optimiste.
C'est déjà très bien si les élèves ont une conjecture étayée par une table.

D'autre part, grâce au chercheur, nous avons eu accès au livre de Gauss "Recherches arithmétiques" traduit en français par Poullet-Delisle, édité chez Courcier Imprimeur de 1807,.

On trouve par exemple dans la proposition 112 une condition sur *p* premier pour que "+2 et -2 soient non-résidus".
Ce document que les élèves n'ont pas utilisé est une mine pour continuer sur ce sujet.
C'est aussi dire que le club n'a rien découvert … à ce jour… mais l'important n'est-il pas de participer ?

En guise d'écho de la part des élèves cette remarque reçue à la rentrée d'une participante envolée en post-bac :

> *Vous nous avez permis de faire un voyage*
> *extraordinaire et magique*
> *dans le monde des mathématiques.*
> *J'en garde un merveilleux souvenir*
> *et souhaite que les générations d'élèves à venir*
> *puissent elles aussi toucher aux maths "autrement".*