Initiation aux équations algébriques modulo un nombre premier Le cas du nombre d'or

Pour les élèves-professeurs, les classes de troisième et seconde avec une initiation pour les plus jeunes.

Cet article fait suite à quatre articles mis en ligne sur notre site IREM par Ruben Rodriguez à destination des professeurs et élèves- professeurs et à notre article des pages précédentes sur les nouvelles notions de "Pentagone et Croix célestes".

Le Nombre d'Or noté en général φ est la racine positive de l'équation : $x^2 + x + 1 = 0$ qui est égale à $\frac{1+\sqrt{5}}{2}$.

Ce nombre, hormis son intérêt historique indéniable est une mine (d'or, excusez le pléonasme !) pour le mathématicien qui trouve son miel dans son étude et peut piocher dans divers champs mathématiques pour concevoir des activités tant de découverte que de consolidation de notions très variées.

Comme le rappelle Antoine Chambert-Loir dans son article de la *Gazette des Mathématiciens* (janvier 2012) Carl Friedrich Gauss s'était déjà intéressé à la résolution d'équations en considérant que tout multiple d'un nombre premier donné est nul. Il s'agit bien entendu de travailler dans les corps finis de la forme $\mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier fixé supérieur ou égal à trois.

Pour le lecteur non familier de l'arithmétique modulaire, nous allons rappeler quelques notions sur les congruences modulo p puis étudier deux cas particuliers $p = 7$ et $p = 11$ dans le cas de la résolution de l'équation caractéristique de φ.

I – Rappel sur les congruences

I - a) L'addition dans $\mathbb{Z}/p\mathbb{Z}$

Rappelons tout d'abord une petite énigme chinoise du Vème siècle citée par A. Chambert-Loir :

Nous avons un nombre inconnu de choses. Si nous les comptons par trois, il en reste deux ; si nous les comptons par cinq il en reste trois, si nous les comptons par sept, il en reste deux. Trouver le nombre de ces choses.

Si cela vous inspire nous vous invitons à chercher une méthode de résolution… Si cela ne vous inspire pas vous trouverez quelques indications en annexe.

Pour notre part nous allons vous définir les congruences et vous proposerons une "chinoiserie" plus simple sous une forme moderne.

Définitions : Soit p est un nombre premier fixé. Dans notre travail, p sera choisi supérieur ou égal à 3.

- On dit qu'un nombre n est congru à zéro modulo p si c'est un multiple de p (p est lui-même un de ses multiples).
- On dit que deux nombres n et m sont congrus modulo p si leur différence $n - m$ est multiple de p.

Ainsi si $p = 7$ alors 14 est congru à 0 modulo 7 , cela s'écrit : $14 \equiv 0 \mod 7$. Et 15 est congru à 1 modulo 7 ce qui s'écrit : $15 \equiv 1 \mod 7$. Si $p = 11$ alors 33 est congru à 0 modulo 11 et 17 est congru à 6 modulo 11.

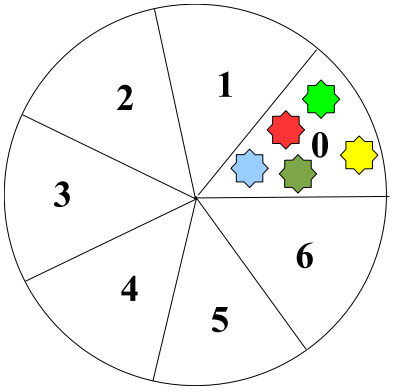
Pour rendre les choses plus perceptibles on peut imaginer que les nombres de 1 à p sont répartis sur une circonférence et que lorsque l'on se déplace sur cette circonférence, quand on arrive en p, c'est " un tour pour rien ".

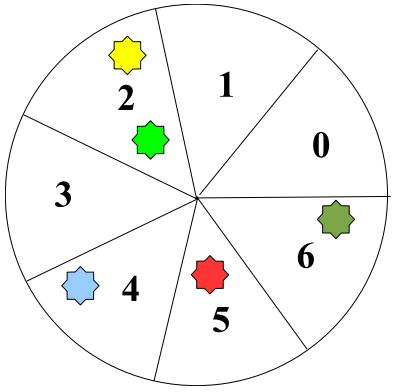
Pour les plus jeunes de nos élèves on peut donc leur proposer le petit jeu suivant :

Matériel : une feuille de papier fort, un compas, un rapporteur, un dés à six faces, des pions de couleurs différentes, par groupe de cinq élèves, par exemple.

Le professeur peut tracer le cercle et les cases numérotées auparavant, sinon :

Tracer sur une feuille un cercle et répartir régulièrement sur sa circonférence sept points notés de 0 à 6 (on peut s'aider du rapporteur). Tracer les rayons associés à ces points pour obtenir des quartiers. On pose les pions de couleurs différentes (un par élève) sur le 0.





Chaque élève lance le dé et place son pion sur le nombre trouvé, il note son score sur un papier.

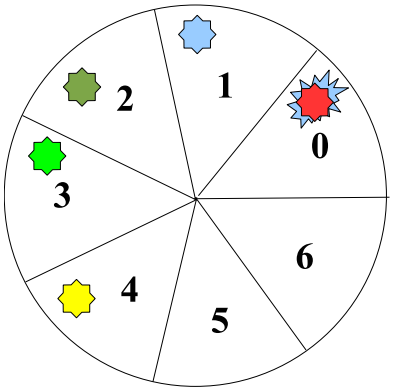
Au tour suivant chacun joue et déplace son pion selon son nombre de points comme aux « petits chevaux ». Chacun note son score, on peut dépasser le 0.

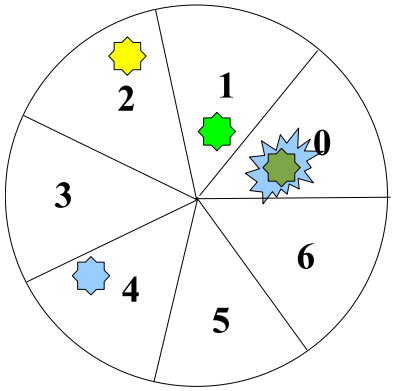
Le premier qui tombe exactement sur 0 a gagné, il enlève son pion, les autres continuent jusqu'à ce qu'ils tombent sur 0. Quand le jeu est fini chacun annonce ses points successifs, on a ainsi plusieurs façons d'obtenir 0 modulo 7.

Nous avons simulé un jeu : au premier tour le vert clair et le jaune ont tiré 2, le bleu a tiré 4, le rouge a tiré 5 et le vert foncé 6. Personne n'a 0 car il n'y a que 6 faces au dé.

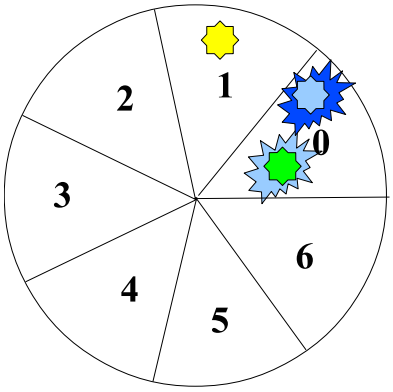
Au second tour (voir figure page précédente) le vert clair a tiré 1, le bleu 4, le jaune et le rouge 2 et il tombe sur le 0 donc il gagne et quitte la partie, le vert foncé a tiré 3, il dépasse le 0 et va en 2.

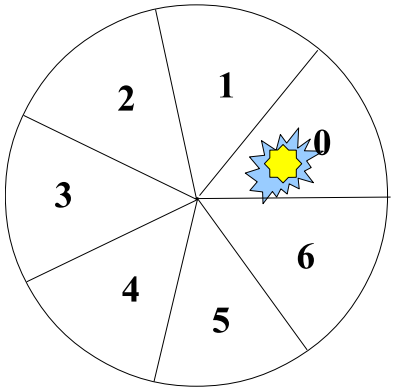
Au troisième tour le vert clair a tiré 5, il dépasse le 0 et passe en 1, le jaune a tiré 5, il dépasse aussi le 0, le bleu a tiré 3, le vert foncé a tiré 5, il tombe sur 0, c'est le deuxième gagnant, il sort du jeu.





Les autres continuent jusqu'à ce qu'ils trouvent 0. Au quatrième tour le vert clair tire 6, il tombe sur le 0, il sort du jeu, le bleu tire 3, il tombe aussi sur 0 et sort du jeu. Le jaune tire le 6 il passe en 1.





Au cinquième tour , le jaune tire encore 6 et tombe en 0. Le jeu est terminé nous écrivons au tableau les scores successifs :

vert clair 2 + 1 + 5 + 6 = 14 GAGNANT !
Jaune 2 + 2 + 5 + 6 + 6 = 21 GAGNANT !
bleu 4 + 4 + 3 + 3 = 14 GAGNANT !
rouge 5 + 2 = 7 GAGNANT !
vert foncé 6 + 3 + 5 = 14 GAGNANT !

Nous récapitulons les résultats :

$2+1+5+6=14\equiv 0 \mod 7$
$2+2+5+6+6=21\equiv 0 \mod 7$
$4+4+3+3=14\equiv 0 \mod 7$
$5+2=7\equiv 0 \mod 7$
$6+3+5=14\equiv 0 \mod 7$

Ce petit jeu fait calculer la somme de différents tirages modulo 7.

Les jeunes ne sachant pas compter modulo 7 peuvent compter les cases comme au jeu des petits chevaux mais ils doivent noter leur score à chaque fois.

Dans cette optique de présentation des nombres entiers modulo p pour les plus jeunes nous vous présentons maintenant quelques « souvenirs didactiques » de Ruben Rodriguez qui, dans les années 1970 a introduit dans son collège de Montevideo, ces notions algébriques. Tous les « anciens » qui ont, soit enseigné ces notions, soit aidé leurs enfants à les apprendre peuvent témoigner que cela les amusait beaucoup (les enfants !) et terrorisait seulement les parents car les IREM en particulier (créés à cette occasion !) élaboraient de multiples jeux pour les introduire auprès des enfants qui ne s'en plaignaient pas, loin de là ! Le professeur André Lichnérowicz, à l'origine de l'introduction de ces notions auprès

des plus jeunes était peut-être un peu trop ambitieux (il présidait de 1966 à 1973 la Commission ministérielle sur l'enseignement des mathématiques qu'il voulait moderniser, ce qui de notre point de vue, fut réalisé de façon trop précipitée : les mathématiques, c'est « de la sueur et des larmes »). Il avait oublié que – avec des jeunes (et les moins jeunes aussi d'ailleurs) – il faut essayer chaque fois que c'est possible de « jouer avec les maths », car les mathématiques sont très ludiques.

I – b) Un autre jeu : témoignage de Ruben sur ses souvenirs de l'introduction des « Maths modernes »

Au cours de mes travaux de recherche en Uruguay sur l'enseignement des mathématiques modernes dans les années 70, que j'appliquais dans mes classes de première année du collège, je créai une situation de jeu avec un ballon et cinq élèves réunis en cercle dans la cour du collège.

Je le nommai « Jeu du distrait ». Il a été analysé didactiquement dans ma thèse de doctorat en Sciences de l'Éducation, mention Didactique des mathématiques, « La pédagogie des mathématiques est-elle moderne ? », sous la direction de Gaston Mialaret soutenue à l'Université de Caen en 1978.

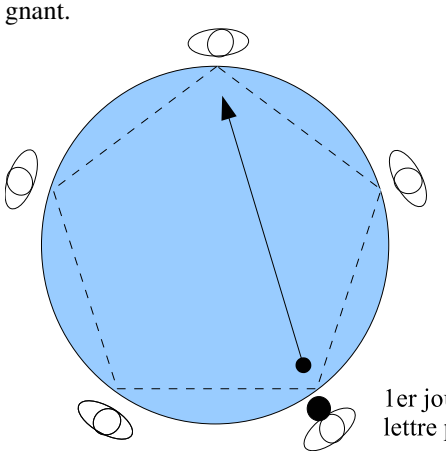
Voici la description de la situation didactique.

1) Dans une première phase les élèves entendaient l'enseignant prononcer une des voyelles parmi **a,e,i,o,u** : L'élève qui avait le ballon dans ses mains devait passer le ballon de la manière suivante :

Pour la voyelle **a** au premier joueur à sa gauche ;

Pour la voyelle **e** au deuxième joueur à sa gauche ;

Pour la voyelle **i** au troisième, pour le **o** au quatrième et pour le **u**, il devait rester avec le ballon dans ses mains. Au bout d'un nombre fixé à l'avance de passages du ballon, l'élève qui se trompait le moins de fois était le gagnant.



2) Dans une deuxième phase l'enseignant prononçait deux voyelles à la suite et les élèves devaient faire le calcul exact avant de faire la passe du ballon.

Par exemple **a a** donnait **e** ;

a e donnait **i** ;

a i donnait **o** ;

a o donnait **u**.

3) Dans une troisième phase les élèves revenaient dans la salle de cours et ils modélisaient le jeu dans sa deuxième phase.

Ceci conduisait au tableau à double entrée suivant :

opération	a	e	i	o	u
a	e	i	o	u	a
e	i	o	u	a	e
i	o	u	a	e	i
o	u	a	e	i	o
u	a	e	i	o	u

4) Plus tard dans une autre séance les élèves travaillaient sur des congruences modulo 2, modulo 3, modulo 4, ensuite ils avaient rencontré la congruence modulo 5.

Les élèves construisaient des tableaux des opérations binaires internes, en particulier le tableau de l'addition modulo 5.

+ modulo 5	1	2	3	4	0
1	2	3	4	0	1
2	3	4	0	1	2
3	4	0	1	2	3
4	0	1	2	3	4
0	1	2	3	4	0

5) Nous avons travaillé à cette époque de « mathématiques modernes » avec nos élèves à Montevideo la notion de morphisme et d'isomorphisme.

C'est ainsi que les élèves nous ont dit qu'il y avait un isomorphisme entre le groupe du « jeu du distrait » et le groupe des nombres entiers modulo 5 parce que c'est le même tableau et donc que les deux opérations fonctionnent de façon similaire.

Il faut dire que ces élèves qui étaient à peu près dans le milieu du troisième trimestre de l'année scolaire avait bien avancé dans le vocabulaire des mathématiques modernes que l'on avait travaillé tout au long de l'année.

Remarque didactique : nous avons découvert à cette époque l'importance didactique du travail des élèves d'abord dans un univers expérimentable, ici il s'agit de l'univers du jeu avec le ballon et ensuite dans un univers morphique formalisant : l'univers de la table des opérations binaires internes. Et aussi dans d'autres univers comme ceux des congruences modulo 2, 3, 4 5, ...

Commentaire : les élèves de Montevideo des ces classes de sixième ont fait à la fin de l'année une exposition avec des affiches et en leur présence pour expliquer aux adultes les mathématiques apprises dans l'année. Il y a eu beaucoup de parents, collègues enseignants et même, l'inspecteur général des mathématiques et le ministre de l'éducation nationale et ils se sont fait expliquer par les élèves, entre autres notions l'isomorphisme cité plus haut !

Il faut souligner que des collègues du secondaire n'avaient jamais travaillé sur les isomorphismes algébriques et encore moins les parents qui n'avaient jamais entendu parler de ceux-ci au cours de leur scolarité.

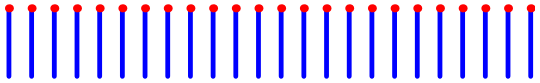
Voici donc le témoignage de cette époque riche en recherches sur la pédagogie des mathématiques, en France avec les IREM et aussi dans d'autres pays comme celui de mes origines, l'Uruguay, où j'avais fondé une équipe de recherche à Montevideo avec des collègues et plus tard avec l'inspecteur général Galli Nari qui avait souhaité participer à titre personnel à nos travaux.

II – Les multiplications dans $\mathbb{Z}/p\mathbb{Z}$

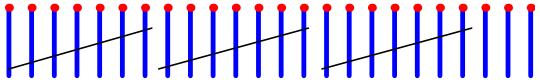
Nous expliquons que l'on peut faire aussi des multiplications des nombres entiers non nuls en décidant que :

« sept égale zéro ».

Pour commencer on dessine sur son cahier un nombre inconnu de petits traits, cette présentation est parfois désignée par « jeu des allumettes » et peut être réalisée avec ces dernières :



Nous demandons aux élèves de faire des paquets de sept traits en les barrant, si on opère avec des allumettes ont les met en paquets de sept :



Dans notre exemple il en reste trois. Ensuite nous leur demandons de compter leurs petits traits, dans notre exemple il y en a 24. Nous écrivons au tableau : 24 égale 3 modulo 7. Nous vérifions que 3 est le reste de la division de 24 par 7. Nous notons au tableau tous les résultats et vérifions que nous avons bien trouvé les restes modulo 7.

Nous allons alors écrire les tables d'addition et de multiplication modulo 7

+	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

Nous voyons donc que lorsque le résultat d'une addition ou d'une multiplication est plus grand que 7 on enlève 7 autant de fois que nécessaire pour trouver un nombre plus petit que 7.

×	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

Nous demandons aux élèves d'observer ces deux tables attentivement et d'observer comment sont répartis les nombres. Ces tables font penser au jeu de sudoku : les nombres entiers de 0 à 6 apparaissent un fois et une seule dans chaque ligne et dans chaque colonne, on dit que l'on a des " Carrés Latins ".

Lorsque l'on définit une opération sur un ensemble, ici par exemple une " addition " sur les nombres entiers de 0 à 6 modulo 7, si la table représentant les résultats des additions pour tout couple de nombres entiers est un carré latin alors l'opération est telle que chaque nombre admet un opposé, c'est-à-dire que pour tout nombre p il existe un nombre q tel que $p + q = 0$, on dit que p est l'opposé de q (dans notre exemple modulo 7) et que q est l'opposé de p. D'autre part le résultat de l'addition de deux nombres entiers quelconques est unique, par exemple, on ne peut avoir à la fois :

$2 + 3 = 5$ et $2 + 3 = 0$ modulo 7.

Si l'opération est une multiplication, il est d'usage de parler d'inverse d'un nombre et non d'opposé, et on dit que p est l'inverse de q si $p \times q = 1$.

Ainsi $2 \times 4 = 1$ modulo 7, on dit que 4 est l'inverse de 2 modulo 7 et aussi que 2 est l'inverse de 4 modulo 7.

III – Les équations à coefficients dans $\mathbb{Z}/p\mathbb{Z}$

III – a) Commençons par résoudre une équation du premier degré à coefficients dans l'ensemble des entiers modulo 7

On suppose que cet ensemble est muni de deux opérations : l'addition et le produit dont les deux tables sont les précédentes.

Résolvons l'équation $2y = 1$ modulo 7.

Nous recherchons dans la table de multiplication un nombre qui multiplié par 2 donne 1, nous observons que $2 \times 4 = 1$ donc $y = 4$ est solution de l'équation.

Résolvons l'équation $3y + 1 = 0$ modulo 7.

Elle équivaut à $3y = 0 - 1 = -1$ modulo 7.

-1 n'apparaît pas dans la table, donc nous devons chercher comment écrire -1 avec un nombre positif. Quelle est la particularité de -1 ? C'est l'opposé de 1 car

$-1+1 = 0$ modulo 7, donc il faut chercher dans la table

d'addition quel est le nombre qui ajouté à 1 donne 0. C'est 6, donc 6 est l'opposé de 1 et $6 = -1$ modulo 7.

Notre équation devient : $3y = 6$ modulo 7. Dans la table de multiplication nous vérifions que $3 \times 2 = 6$, la solution est donc $y = 2$.

Les équations du premier degré sont donc assez simples à résoudre. Nous passerons plus loin aux équations du second degré.

III – b) D'autres équations modulo 7 sont amusantes à résoudre

Elles donnent à réfléchir dans un domaine que l'on appelle l'arithmétique, par exemple :

Essayons de résoudre l'équation : $2y \equiv 3z \mod 7$. Nous voyons que nous devons chercher deux nombres entiers y et z dans la table de multiplication tels que 2 fois l'un vaut 3 fois l'autre...Nous voyons que :

$2 \times 3 = 6 = 3 \times 2$ donc $y = 3$ et $z = 2$ conviennent.

Y-a-t-il d'autres possibilités ? Nous remarquons par exemple que :

$2 \times 5 = 3 = 3 \times 1$; donc $y = 5$ et $z = 1$ conviennent.

En fait si nous continuons ainsi nous voyons que pour tout y de notre ensemble des entiers modulo 7 il existe un z tel que $3y \equiv 4z \mod 7$. Pourquoi ?

Nous avons observé plus haut que tout élément de l'ensemble admet un inverse donc nous pouvons transformer notre équation :

$2y \equiv 3z \mod 7$ en $y = (1/2) \times 3z$. Nous devons rechercher le nombre qui multiplié par 2 donne 1 c'est 4 donc l'équation devient : $y = (1/2) \times 3z \equiv 12z \mod 7$, soit encore $y = 5z$, donc pour tout z de 1 à 6, il suffit de choisir pour y la valeur z multipliée par 5.

Les couples de nombres entiers solutions de l'équation sont donc :

(5,1) ; (3,2) ; (1,3) ; (6,4) ; (4,5) ; (2,6).

III – c) Les équations du second degré

Par exemple l'équation $y^2 = 4$ a deux solutions évidentes $y = 2$ et $y = -2 \equiv 5 \mod 7$.

Mais l'équation $y^2 = 3$ a-t-elle une solution ? Nous n'avons pas trouvé de nombre qui multiplié par lui-même donne 3. Observons dans la table de multiplication si d'autres nombres entiers admettent une racine.

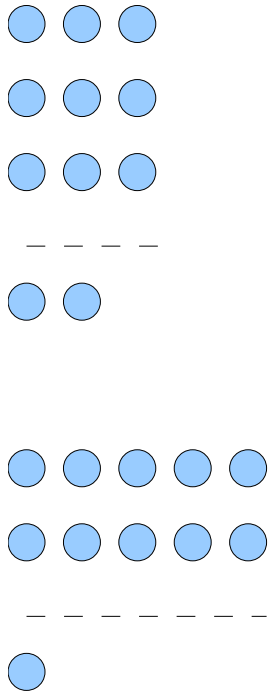
Nous avons $1 \times 1 = 1$ donc 1 admet sa racine habituelle 1, mais aussi :

$6 \times 6 = 1$ donc 6 est aussi racine de 1. Est-ce surprenant ? Non car $6 = -1$.

Récapitulons : l'ensemble des nombres entiers modulo 7 que nous noterons $\mathbb{Z}/7\mathbb{Z}$ admet deux racines carrées : racine (1) et racine (6).

IV – Entracte : une énigme plus simple que celle des Chinois

J'ai dans ma poche des pièces de 1 €, si je les compte par trois il en reste deux, si je les compte par cinq il en reste une, combien ai-je de pièces ?



Observons la première équation qui exprime que lorsque l'on divise P, nombre de pièces, par 3 il reste 2.
Observons la deuxième : lorsque l'on divise P par 5 il en reste une.
Peut-on utiliser la deuxième pour améliorer la première ?
Multiplions la première par 5, on obtient :
$5P = 15n + 10$. Multiplions la deuxième par 3 on obtient :
$3P = 15m + 3$. Soustrayons les deux expressions :
$2P = 15(n - m) + 7$, ce qui se dit aussi
$2P$ est congru à 7 modulo 15. Nous avons maintenant une seule congruence.
Essayons le cas où $m = n$ alors $2P = 7$ ce qui est impossible car 7 n'est pas un nombre pair, essayons $n - m = 1$ alors :
$2P = 22$ et $P = 11$, est-ce possible ? Oui car :
$11 = 3 \times 3 + 2$ et $11 = 2 \times 5 + 1$

J'ai 11 pièces dans ma poche.

V – Le cas nombre d'or φ, solution de l'équation à coefficients entiers : $y^2 - y - 1 = 0$.

On peut se demander si le nombre d'or a un sens dans $\mathbb{Z}/7\mathbb{Z}$ puisque les coefficients de l'équation dont φ est solution sont 1 et 0.

On peut étudier ce problème de deux façons différentes :

- L'approche par essais successifs ;
- L'approche algébrique habituelle dans les nombres réels. Commençons par cette dernière :

On sait que dans l'ensemble des nombres réels φ s'écrit : $\varphi = \dfrac{1+\sqrt{5}}{2}$.

Nous avons vu que $\sqrt{5}$ n'existe pas dans $\mathbb{Z}/7\mathbb{Z}$. Ne nous décourageons pas, on ne sait jamais...
Essayons les éléments successifs de $\mathbb{Z}/7\mathbb{Z}$.

$y = 0$ ne convient pas ; y = 1 ne convient pas ;
$y = 2$, on a $4 - 2 - 1 \equiv 0$;
$y = 3$, on a : $9 - 3 - 1 = 2 - 3 - 1 = 5 \equiv 0$;
$y = 4$, on a : $16 - 4 - 1 = 4 \equiv 0$;
$y = 5$, on a : $25 - 5 - 1 = 5 \equiv 0$;
$y = 6$, on a : $36 - 6 - 1 = 1 \equiv 0$.

Le nombre d'or n'existe donc pas dans $\mathbb{Z}/7\mathbb{Z}$, bien que 7 soit traditionnellement " un nombre sacré " (!).

Le cas des entiers modulo 11

Antoine Chambert-Loir, dans son article de la "Gazette des mathématiciens" nous propose d'étudier l'équation du nombre d'or dans l'ensemble des entiers modulo 11 : $\mathbb{Z}/11\mathbb{Z}$.

L'addition s'effectue, comme dans les entiers modulo 7 mais il y a maintenant 11 éléments, numérotés de 0 à 10.

La multiplication présente les mêmes caractéristiques que la multiplication modulo 7, en particulier tout élément admet un inverse. (voir la table ci-dessous)

Nous demandons aux élèves de construire la table de multiplication seuls afin de bien installer ces techniques de calcul et de raisonnement dans un contexte inhabituel.

Tout d'abord essayons comme précédemment de chercher si la racine de 5 existe dans cet ensemble. Autrement dit existe-t-il un nombre qui multiplié par lui-même donne 5 ? Nous constatons que $4^2 = 5$ et $7^2 = 5$.

Remarquons que les deux nombres entiers 4 et 7, (4 + 7 = 0 modulo 11) sont opposés et que cette propriété algébrique est générale : il existe deux racines de 5. Comme dans les nombres relatifs il y a deux racines, on convient dans ceux-ci de choisir la racine positive mais dans $\mathbb{Z}/11\mathbb{Z}$ cela n'a pas de sens puisque tout nombre est à la fois positif et négatif.

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	1	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

Donc nous allons vérifier si au moins l'une des solutions $\frac{1+4}{2} = \frac{5}{2}$ ou $\frac{1+7}{2} = \frac{8}{2}$ convient.
Or est 8 le nombre qui multiplié par 2 donne 5.

Le nombre d'or dans l'ensemble des nombres entiers modulo 11 est-t-il 8 ?

Nous devons chercher si $8^2 - 8 - 1 = 0$ soit $9 - 8 - 1 = 0$, ce qui est vérifié. Le nombre d'or modulo 11 est 8.
Étudions la deuxième solution $8/2$. Notre premier mouvement nous incite à poser $\frac{8}{2} = 4$
Effectuons le calcul $4^2 - 4 - 1 = 5 - 4 - 1 = 0$;
Un second nombre d'or modulo 11 est 4, cette solution convient.

Pour consolider les résultats nous demandons aux élèves de faire les calculs pour tous les nombres entiers de $\mathbb{Z}/11\mathbb{Z}$.
L'existence de deux nombres d'or dans l'ensemble des entiers modulo 11 nous interpelle et nous incite à nous poser des questions intéressantes...

Tout d'abord ces résultats ont-ils un sens géométriquement ? Peut-on imaginer que dans $\mathbb{Z}/11\mathbb{Z}$, il y ait une « divine proportion » ?

Par exemple observons le couple de nombre (1,8), le couple suivant délivré par une « suite à la Fibonacci »(c'est-à-dire une suite de Fibonacci généralisée) est (8,9) est-il dans la même proportion ?

A-t-on : 8/1 = 9/8 modulo 11 ?

Nous avons prouvé précédemment que si trois nombres a, b, c vérifient $c = a + b$ et que $b/a = c/b$, ceci équivaut à $b/a = \varphi$, effectuons le calcul pour vérifier cette assertion.
Nous observons dans la table de multiplication modulo 11 que $9/8 = 8$, ce qui convient.

Le « deuxième » nombre d'or modulo 11 est 4.

Le premier couple est donc (1,4) le deuxième (4,5), or $5/4 = 4$, ce qui convient.

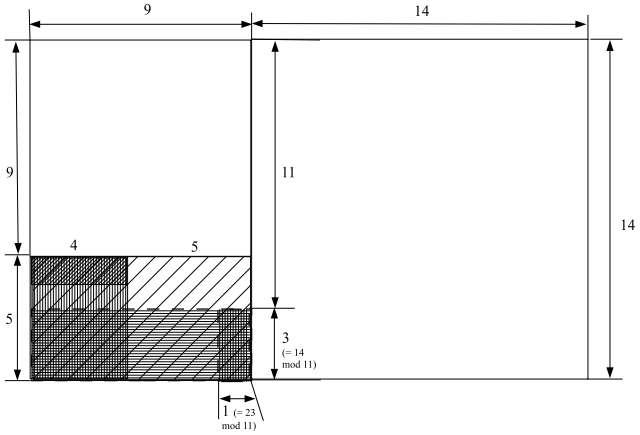
Nous pouvons essayer de représenter cet « univers modulo 11 », qui est ce que l'on appelle un univers « discret » (c'est-à-dire opposé à continu) une construction de la spirale des rectangles d'or successifs : les « dimen-

sions » des rectangles d'or successifs, construits comme dans les nombres réels, comme une suite de Fibonacci sont : (1 ; 4) ; (4 ; 5) ; (5 ; 9) ; (9 ; 14) soit (9 ; 3) modulo 11 ; (3 ; 12) soit (3 ; 1) modulo 11 ; (1 ; 4) et nous revenons au rectangle d'origine.

Nous vérifions que
3/9 = 4 modulo 11 et que 1/3 = 4 modulo 11. les « rectangles d'or » ont leurs côtés proportionnels au « nombre d'or » 4. Il y a donc cinq « rectangles d'or modulo 11 » distincts correspondants au nombre d'or modulo 11 soit 4, ce sont les couples :

(1 ; 4) ; (4 ; 5) ; (5 ; 9) ; (9 ; 3) et (3 ; 1) on retrouve ensuite (1 ; 4).

Nous avons dessiné en tirets gras les rectangles d'or modulo 11 « écrasés », tous les rectangles d'or modulo 11 sont inscrits dans le rectangle (5 ; 9).



Observons maintenant cela avec 8, « nombre d'or modulo 11 ».

Les couples de nombres entiers correspondants à une suite de Fibonacci généralisée sont :

(1 ; 8) ; (8 ; 9) ; (9 ; 6) ; (6 ; 4) ; (4 ; 10) ; (10 ; 3) ; (3 ; 2) ; (2 ; 5) ; (5 ; 7) ; (7 ; 1) ; on retrouve ensuite (1 ; 8).

VI – Quelques remarques pour les élèves-professeurs

Il n'est pas innocent d'avoir choisi pour nos exemples des nombres entiers modulo un nombre premier. En effet la théorie de Galois montre que les ensembles de nombres entiers modulo p premier se munissent facilement d'une structure de corps commutatif et, de ce fait, se prêtent bien à la résolution des équations.

D'une façon générale, si nous voulons résoudre des équations du second degré nous devons chercher si un nombre a de $\mathbb{Z}/p\mathbb{Z}$ est un carré. Nous dirons qu'alors « a est un résidu quadratique modulo p ».

Les corps $\mathbb{Z}/p\mathbb{Z}$ sont cycliques c'est-à-dire qu'un élément α est générateur du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$:
$(\mathbb{Z}/p\mathbb{Z})^* = \{1, \alpha, \alpha^2, \alpha^3, \ldots . \alpha^{p-2}\}$.

On a alors le théorème suivant : $\alpha^{\frac{p-1}{2}} \equiv -1 \mod p$

Soit un nombre premier impair. **Un générateur α n'est pas un résidu quadratique**. En effet d'après le petit théorème de Fermat on a $\alpha^{p-1} = 1$ donc, $\alpha^{\frac{p-1}{2}} = \pm 1$.

Puisque α est un générateur la seule solution possible est : $\alpha^{\frac{p-1}{2}} = -1$

Si α était un carré on aurait $\alpha = \beta^2$ et $\alpha^{\frac{p-1}{2}} = \beta^{p-1} = 1$, ce qui est faux puisque α étant générateur son ordre est exactement $p - 1$.

Deuxième théorème

Dans un corps $\mathbb{Z}/p\mathbb{Z}$ les seuls résidus quadratiques sont les puissances paires d'un générateur.

En effet il est clair que les nombres entiers de la forme α^{2k} sont des carrés, d'autre part si α^{2k+1} était un carré de la forme u^2 on aurait $\alpha = \dfrac{u^2}{\alpha^{2k}}$ et α serait un carré, ce qu'il n'est pas.

Reprenons le cas que nous avons traité précédemment où $p = 11$, nous avons vu que 5 admet deux racines carrées dans $\mathbb{Z}/11\mathbb{Z}$: 4 et 7 (ou -4), ce qui semble pour le moins surprenant car 5 n'est pas une puissance paire d'un générateur ! Remarquons tout d'abord que 11 étant premier, $\mathbb{Z}/11\mathbb{Z}$ est un corps cyclique donc son groupe multiplicatif admet un générateur.

Par exemple 2 est générateur. Vérifions-le :
$2^2 = 4$; $2^3 = 8$; $2^4 = 16 \equiv 5 \mod 11$;
$2^5 = 32 \equiv 10 \mod 11$; $2^6 = 64 \equiv 9 \mod 11$;
$2^7 = 128 \equiv 7 \mod 11$; $2^8 = 256 \equiv 3 \mod 11$;
$2^9 = 512 \equiv 6 \mod 11$; $2^{10} = 1024 \equiv 1 \mod 11$.

Tous les nombres entiers modulo 11 peuvent s'exprimer comme une puissance de 2. Nous remarquons dans la table de multiplication que $5 = 2 \times 8 = 16$ et $16 = 2^4$. Ce qui nous satisfait...

Nous pouvons observer la diagonale sur la table de multiplication de $\mathbb{Z}/11\mathbb{Z}$: les carrés (en rouge) se trouvent sur celle-ci, ce sont : 1, 3, 4, 5, 9.
$1 = 1^2 = 10^2$; $3 = 5^2 = 6^2$; $4 = 2^2 = 9^2$;
$5 = 4^2 = 7^2$; $9 = 3^2 = 8^2$.

Vérifions que ces carrés, sauf 1 sont des puissances paires de 2 :
$4 = 2^2$; $3 = 4 \times 9 = 2^2 \times 2^6 = 2^8$; $5 = 2 \times 8 = 2^4$;
$9 = 8 \times 8 = 2^6$.

Réciproquement, existe-t-il des nombres entiers dans $\mathbb{Z}/11\mathbb{Z}$ qui ne sont pas des carrés parfaits ? (à part 2 qui étant générateur ne peut être un carré).

Ce sont les autres nombres : 2, 6, 7, 8, ce dernier est une puissance impaire de 2.

Une remarque à propos des « rectangles d'or modulo 11 que nous avons calculés précédemment, nous

remarquons que nous avons seulement 5 rectangles d'or correspondants au « nombre d'or modulo 11 » : 4 alors que nous avons 10 rectangles d'or correspondants au « nombre d'or modulo 11 » : 8. Comment expliquer cette différence ?

Notre intuition nous souffle que cela est dû au fait que 4 n'est pas un générateur modulo 11 car c'est un carré alors que 8 est générateur car c'est une puissance impaire du générateur 2 (deuxième théorème).

Essai de généralisation

Soit p un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ le corps quotient correspondant. Nous voulons chercher si $\sqrt{5}$ existe dans ce corps, autrement dit, existe-t-il un nombre q pair inférieur à p tel que $2^q \equiv 5 \bmod p$? Est-ce une condition nécessaire et suffisante ? Nous allons voir qu'elle est seulement suffisante. Essayons par exemple le nombre premier $p = 17$; les calculs sont fastidieux, nous essayons de tracer des courbes $y = 2^x$ et $y = 17x$ avec GEOGEBRA mais la recherche est peu efficace à cause du peu de précision des calculs. Nous cherchons sur internet la liste des nombres premiers jusqu'à 100 000 que nous trouvons sur le site web en note[1].

Ensuite nous écrivons dans un tableau les puissances paires de 2 auxquelles nous ajoutons ou retranchons 5. Nous recherchons si le nombre trouvé est premier, nous trouvons ainsi que 5 est un carré dans les corps : $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/59\mathbb{Z}$, $\mathbb{Z}/251\mathbb{Z}$, $\mathbb{Z}/1039\mathbb{Z}$, $\mathbb{Z}/4901\mathbb{Z}$, $\mathbb{Z}/74901\mathbb{Z}$.

Cette méthode nous semble incomplète, pouvez-vous en trouver d'autres ? Si le sujet vous intéresse, vous pouvez trouver des résultats concernant la recherche de racines carrées dans les corps, sur le site web en note[2].

Plus généralement, grâce à l'aide de notre collègue Christian Ballot de l'Université de Caen, écrivons comment on peut trouver tous les corps modulo p admettant une racine carrée de 5. Ce résultat provient de la loi de réciprocité quadratique étudiée particulièrement par Gauss (en 1801). Appliquons cette loi à 5 :

5 est un carré modulo p si et seulement si $p \equiv \pm 1 \bmod 5$.

Annexe : le problème chinois

Nous avons un nombre inconnu de choses. Si nous les comptons par trois, il en reste deux ; si nous les comptons par cinq il en reste trois, si nous les comptons par sept, il en reste deux. Trouver le nombre de ces choses. Ainsi, en notant a le nombre des choses :

$a = 2 \bmod 3$; $a = 3 \bmod 5$; $a = 2 \bmod 7$. Écrivons ces équations en éliminant l'inconnue a ; nous avons :
$2 \mod 3 = 3 \mod 5 = 2 \mod 7$ soit encore :

$2 + 3r = 3 + 5s = 2 + 7t$ où r, s, t sont des entiers que nous pouvons choisir positifs. Nous en déduisons : $3r = 7t$; puisque 3 et 7 sont premiers entre eux nous en déduisons que 3 divise t et 7 divise r ; $r = 1$ et $s = 1$ ne conviennent pas, essayons $t = 3$ et $r = 7$ alors $3 + 5s = 23$; $s = 4$.

D'où $a = 23 = 3 \times 7 + 2 = 4 \times 5 + 3 = 7 \times 3 + 2$. Nous avons 23 choses.

Bien entendu nous avons traité ce problème en « arithmétique à l'ancienne » afin de ne pas décourager le lecteur non familier avec l'algèbre des structures. En complément on pourra consulter l'article collectif de l'IREM de Toulouse, présenté dans la bibliographie ci-dessous.

Bibliographie

Antoine Chambert-Loir « De Galois aux corps finis », *Gazette des mathématiciens* 131 (2012) p. 58-68.
Ruben Rodriguez Herrera *Activités variées autour du nombre d'or pour la classe de troisième*, quatre articles en ligne sur le site de l'IREM de Basse-Normandie Caen 2012 : http://www.math.unicaen.fr/irem/

Denis Daumas, Michel Guillemot, Olivier Keller, Raphaël Mizrahi, Maryvonne Spiesser *Le théorème des restes chinois. Textes, commentaires et activités pour l'arithmétique au lycée*

Les problèmes de congruences simultanées sont connus dans l'histoire des mathématiques comme « problèmes des restes » ou « des restes chinois ». C'est un sujet qui a donné lieu, depuis des siècles, à de riches développements mathématiques et dont l'origine reste hypothétique puisqu'il est très difficile de démêler les motivations premières qui en ont suscité l'intérêt…

Dossier disponible en téléchargement sur le site http://culturemath.ens.fr et édité en version papier par l'IREM de Toulouse, Université Paul-Sabatier (UFR MIG).

À paraître prochainement la brochure *Recueil d'activités sur le Nombre d'Or* proposée par **Ruben Rodriguez, Danielle Salles, Éric Lehman, Michel Soufflet.** 140 p. environ Éditeur IREM de Basse-Normandie.

[1] http://compoasso.free.fr/primelistweb/page/prime/liste_online.php
[2] http://www.acrypta.com/telechargements/fichecrypto_210.pdf