Master de didactique des mathématiques

UE 3.4

Actualité de la recherche en mathématiques

François MOUSSAVOU

Sous la direction de :

Christian MAUDUIT

Sommaire

Présentation du sujet

Le principe de l'exercice.

Se mettre en situation de recherche sur un problème mathématique ouvert et observer la spécificité de ce type d'activité par rapport à une activité standard de résolution de problème.

Analyse a priori.

Les deux principales différences attendues :

- L'absence de contrainte de temps pour la recherche.
- La possibilité de faire cohabiter ou alterner plusieurs domaines des mathématiques dans le travail de recherche et de résolution.

Une question se pose aussi : comment gère-t-on une activité mathématique où l'on ne produit « rien », ni résultat juste, ni résultat faux ?

Choix du sujet : Les nombres premiers.

Ce choix est essentiellement motivé par deux raisons : l'intérêt personnel que je porte au sujet et le fait que c'est une notion absente des programmes de la totalité des classes de lycée professionnel (tous niveaux, spécialités et filières confondus). Je n'ai donc jamais travaillé sur les nombres premiers en tant qu'enseignant.

Première approche

L'idée est de s'intéresser à un problème non résolu en rapport avec les nombres premiers ; mon choix s'est rapidement porté sur la conjecture de GOLDBACH : la simplicité de l'énonce laissant présager qu'il serait facile de se l'approprier et de commencer à chercher d'une part et que la solution était forcement suffisamment complexe pour laisser un champ d'investigation très vaste.

La première approche s'est avérée décevante :

- Il n'a pas du tout été facile de commencer une recherche.
- L'activité peut se résumer ainsi : une application à l'environnement de la conjecture de GLODBACH, des domaines mathématiques étudiés en cours à ce moment-là (***Annexe 1*** : premières recherches).

Les explications de Christian MAUDUIT m'ont permis, dans un premier temps, de comprendre pourquoi ce choix ne pouvait pas être en adéquation avec le cadre de travail que je m'étais fixé, puis de définir une nouvelle problématique.

Conjecture de GOLDBACH (1742) :

Tout entier pair supérieur à 3 est somme de deux nombres premiers.

Un résultat lié à la conjecture de GOLDBACH : **Le théorème de CHEN** (1966) :

Tout entier pair suffisamment grand est somme d'un nombre premier et d'un nombre semi-premier

(semi-premier : nombre produit de deux nombres premiers – Exemple : 4 ;6 ;9 ;10 ;14 ;15…)

Le 13 mai 2013, le mathématicien péruvien **Harald Andrés HELFGOTT** soumet une preuve de :

La conjecture faible de GOLDBACH (ou conjecture impaire) :

Tout entier impair supérieur à 9, est somme de trois nombres premiers impairs.

Redéfinition du sujet

Le théorème d'EUCLIDE sur l'infinité des nombres premiers peut se démontrer d'un grand nombre de façons. Parmi les différentes preuves, EULER propose de démontrer que la série des inverses de nombres premiers est divergente. En 1919, le mathématicien norvégien Viggo BRUN tente de réutiliser cette méthode pour prouver l'infinité de l'ensemble des nombres premiers jumeaux. Surprise : la série $\sum_{\substack{p\in\mathbb{P}\\ p+2\in\mathbb{P}}} \left(\frac{1}{p}+\frac{1}{p+2}\right)$ converge (vers la constate de BRUN).

Conjecture des nombres premiers jumeaux :

Il existe une infinité de nombres premiers p tels que $p+2$ soit premier.

Présentation du sujet :

- Chercher de nouvelles démonstrations du théorème d'EUCLIDE sur l'infinité des nombres premiers.
- Appliquer les méthodes utilisées dans ces nouvelles démonstrations à la conjecture des nombres premiers jumeaux.

L'idée :

- Produire une démonstration du théorème d'EUCLIDE à l'aide du théorème de WILSON.
- Trouver une caractérisation des nombres premiers jumeaux utilisant le théorème de WILSON.
- Appliquer ces résultats à la conjecture des nombres premiers jumeaux.

Théorème de WILSON :

p premier si et seulement si : $(p-1)! + 1 \equiv 0\ [p]$

Pourquoi partir sur cette idée ?

- Le théorème de WILSON permet de caractériser les nombres premiers mais ne peut pas être utilisé comme test de primarité à cause de la croissance de la fonction factorielle. C'est donc un bon candidat pour obtenir un résultat global sur l'ensemble des nombres premiers (ou plus précisément, c'est un très mauvais candidat pour étudier et calculer sur des nombres spécifiques).
- Aucune des démonstrations du théorème d'EUCLIDE présente dans la liste, non exhaustive, que l'on veut étudier, ne repose sur l'utilisation du théorème de WILSON.

Travail à effectuer :

- Étudier les différentes preuves du théorème d'EUCLIDE. ***Annexe 2*** *: Quelques preuves classiques du théorème d'EUCLIDE sur l'infinité des nombres premiers.*
- Étude de la différence entre les notions d'infini potentiel et d'infini actuel utilisées dans les preuves du théorème d'EUCLIDE. ***Annexe 3*** *: L'infini en mathématiques.*
- Établir l'indépendance des théorèmes d'EUCLIDE et de WILSON. ***Annexe 5*** *: Independence des théorèmes d'EUCLIDE et de WILSON*
- Démontrer le théorème d'EUCLIDE en utilisant le théorème de WILSON. ***Annexe 4*** : Recherches de la deuxième approche.
- Trouver une caractérisation des nombres premiers jumeaux à l'aide du théorème de WILSON. ***Annexe 6*** *: théorème de CLEMENT*

Premières conclusions

L'importance du choix du sujet de recherche :

On s'aperçoit qu'avoir un problème ouvert dont on comprend bien l'énoncé et de la motivation pour chercher, n'est pas suffisant pour se lancer dans ce type de travail : le choix d'un sujet adapté à ses connaissances et ses capacités est fondamental.

Si l'on voulait reproduire cette démarche dans le cadre d'un enseignement standard en classe, il faudrait donc être capable de définir des sujets adaptés aux élèves ; la base *maths en jeans* semble être une très bonne piste pour cela.

L'idée de chercher des nouvelles preuves d'un résultat déjà démontré et une activité très riche et à laquelle je n'aurais pas pensé.

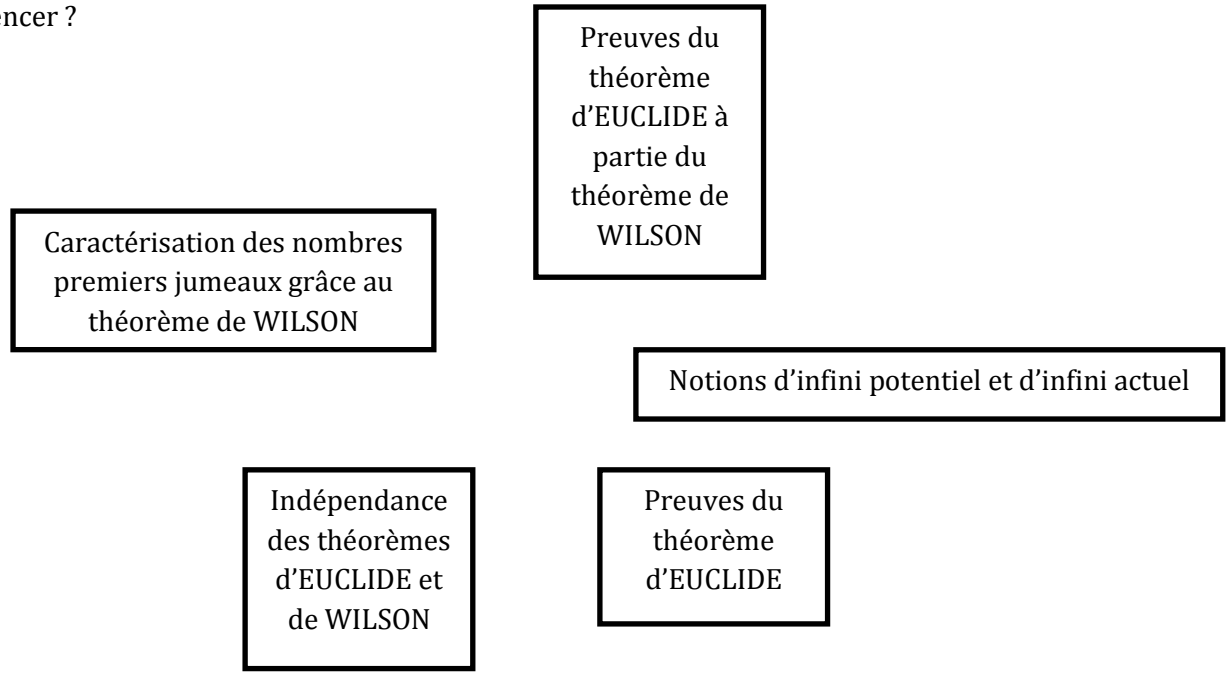
Un phénomène de contrat :

Il est difficile de se lancer dans un travail de réflexion sur un problème non résolu ; le contrat didactique habituel indique à l'élève que le problème a une solution et qu'il a les moyens de la trouver. Là, on se trouve dans la situation inverse : l'environnement semble vous dire qu'il y a peut-être une solution mais qu'elle est, a priori, hors de votre portée.

Il faut donc, dans un premier temps, passer outre cette inhibition pour pouvoir se lancer dans l'activité de recherche. Une solution est de se convaincre que ce qui va être générateur de sens, ce ne sera pas de trouver mais de chercher. Pour réussir cela, il faut structurer sa recherche et on peut en particulier essayer de bien faire ressortir les impasses auxquelles on arrive en leur donnant une sorte de statut de résultat.

Sur l'organisation du travail :

Le travail à effectuer se découpe assez bien en parties distinctes. La question qui se pose alors est : par quelle partie commencer ?



La méthode retenue sera de travailler sur les cinq parties de façon indépendante, même si les différentes phases de travail peuvent être amenées à mutuellement s'influencer.

Ce questionnement m'a conduit à m'interroger sur l'utilité de découper les problèmes de mathématiques en parties (indépendantes ou pas) et à la façon dont ce découpage est fait. Lorsque je crée un problème pour mes élèves, les différentes parties correspondent soit à l'utilisation de domaines ou d'outils mathématiques ciblés, soit à une gradation de la difficulté des questions posées. Ici, on est, a priori, dans aucun de ces deux cas.

Processus d'autocontrôle :

Un autre phénomène observé lors de cette phase de recherche est l'absence de *processus d'autocontrôle* : lorsque je suis en train de chercher la solution d'un exercice ou d'un problème, je sais que si ce que j'écris devient trop long et/ou trop complexe, alors : soit je suis en train de me tromper, soit il existe une solution plus simple que je n'ai pas vue ; je peux donc à tout moment, à travers cela, contrôler la pertinence de ce que je fais. Dans l'activité de recherche sur un problème ouvert, cette méthode d'autocontrôle disparaît totalement.

Cela constitue une vraie différence entre une activité de résolution de problème et une activité de recherche sur une question ouverte. Ce sera pour moi l'un des plus gros enseignements de ce travail ; il aura d'autant plus été mis en relief que : premièrement je ne l'avais pas anticipé (cela ne faisait pas partie de mon *analyse a priori*), deuxièmement je n'avais encore jamais réalisé à quel point le processus d'autocontrôle dans la résolution d'exercices était un outil puissant et constamment sollicité. On peut le voir comme une conséquence du contrat didactique et il mériterait d'être explicité aux élèves qui n'en auraient pas conscience.

Rechercher sans trouver :

Dernier point, la partie recherche de ce travail n'a pas abouti. Même si le fait de travailler sur les quatre autres parties a été très enrichissant et si le fait, comme explicité dans le deuxième paragraphe de cette section, de bien identifier le moment de la recherche où l'on se trouve *bloqué*, permet d'avoir l'impression de produire quelque chose, l'absence de résultat reste frustrante.

Quoiqu'il en soit, si l'on veut transposer ce genre d'activité dans une classe, il me semble nécessaire de prévoir de toujours la faire déboucher sur une production concrète : soit une mise en relief des points de blocage, comme ici, soit la réalisation de posters comme lors des stages *Hippocampe*.

Une preuve de l'infinité des nombres premiers utilisant le théorème de Wilson

Ce travail correspond à une reprise de l'étude. Il est séparé de plus de trois semaines de la fin du premier travail effectué après la redéfinition du sujet.

Raisonnement par l'absurde :

Soit $\mathbb{P}$ l'ensemble des nombres premiers.

On suppose $\mathbb{P}$ fini. On peut alors définir p_M : le plus grand des nombres premiers.

On pose : $\mathbb{N}_M = \{n \in \mathbb{N} \text{ et } n > p_M\}$ et on définit la fonction f :

$$f : \begin{cases} \mathbb{N}_M \to \mathbb{Q} \\ n \mapsto \frac{(n-1)!+1}{n} \end{cases}$$

Par hypothèse : f ne peut pas prendre de valeurs entières

Montrons que : $\forall\, n \in \mathbb{N}_M : n \wedge (n-1)! + 1 = 1$

Soit ***m*** un diviseur commun de ***n*** et (***n***-1) !+1. ***m*** < ***n*** sinon, d'après le théorème de Wilson : ***n*** serait premier.

Donc : $m \mid (n-1)!$ Or : $m \mid (n-1)! + 1$ d'où $m \mid 1$ et donc $m = 1$

On a montré que : $\forall\, n \in \mathbb{N}_M : n \wedge (n-1)! + 1 = 1$

On considère maintenant le nombre : $p_M ! \in \mathbb{N}_M$ .donc : $p_M ! \wedge (p_M ! - 1)! + 1 = 1$. Or $p_M !$ est divisible par tous les nombres premiers et $(p_M ! - 1)! + 1 > p_M$ devrait être divisible par au moins un nombre premier : il a **contradiction**.

Théorème de CLEMENT :

Le théorème de CLEMENT est une caractérisation des nombres premiers jumeaux utilisant le théorème de WILSON. Je l'ai trouvé dans une publication de janvier 1949 lorsque je faisais une recherche sur Internet sur le théorème de WILSON.

> Condition nécessaire et suffisante pour que deux entiers p et p+2 soient tous les deux premiers:
>
> $$4((p-1)!+1)+p \equiv 0\ [p\ (p+2)]$$

Il n'est a priori pas exclu que le théorème de WILSON puisse donner d'autres caractérisations des nombres premiers jumeaux, mais on ne poursuivra pas cette recherche lors de la reprise de l'étude ; le travail de recherche d'une caractérisation des nombres premiers jumeaux se transforme donc en travail d'étude de la preuve de P.A. CLEMENT : ***Annexe 6*** : *Théorème de CLEMENT*.

Retour sur la conjecture des nombres premiers jumeaux

L'idée : appliquer le raisonnement utilisé pour démontrer l'infinité des nombres premiers grâce au théorème de WILSON, à une démonstration de l'infinité des nombres premiers jumeaux grâce au théorème de CLEMENT.

On va supposer que l'ensemble des nombres premiers jumeaux est fini.
On commence par définir le même type d'objets :

$\boldsymbol{p}^*$: le plus grand des nombres premiers tel que : $\boldsymbol{p}^* + 2$ est non premier.
$\mathbb{P}^*$: l'ensemble des nombres premiers strictement supérieurs à $\boldsymbol{p}^*$

$$f : \begin{cases} \mathbb{P}^* \to \mathbb{Q} \\ p \mapsto \dfrac{4\left((p-1)!+1\right)+p}{p(p+2)} \end{cases}$$

Théorème de WILSON $\Rightarrow p \mid (p-1)! + 1$ donc $f(p) = \dfrac{\frac{4\left((p-1)!+1\right)}{p}+1}{p+2} = \dfrac{a_p}{b_p}$

On veut montrer la propriété suivante : ***Propriété*** : $\forall p \in \mathbb{P}^* : (p+2) \wedge (4\frac{(p-1)!+1}{p} + 1) = 1$

Une rapide étude au tableur permet de se convaincre que ce résultat peut être vrai :

p	*p+2*	*Wilson-Clement*	*pgcd*
2	4	5	1
3	5	5	5
5	7	21	7
7	9	413	1
11	13	1319565	13
13	15	147385109	1
17	19	4,92301E+12	19
19	21	1,34787E+15	1
23	25	1,95478E+20	#NOMBRE!

Première idée : établir le résultat intermédiaire suivant :

Lemme : $m \mid p+2 \Rightarrow m \mid (4\frac{(p-1)!+1}{p})$.

Comme $m \mid (4\frac{(p-1)!+1}{p} + 1)$, cela impliquera que $m \mid 1$ et donc $m = 1$. Mais là par contre, le tableur permet d'invalider immédiatement cette hypothèse.

p+2	*m*	*m'*	**(Wilson-Clement - 1)/4**
9	3		103
15	3	5	36846277
21	3	7	3,36967E+14

Démonstration de la propriété :

Soit p un élément de $\mathbb{P}^*$ et m un diviseur strict de $p+2$: $m \mid p+2$ et $m < p+2$. m est impair car p est dans $\mathbb{P}^*$.
Si m est également un diviseur de $(4\frac{(p-1)!+1}{p}+1)$ alors :

p ne divise pas m, sinon, p diviserait aussi $p+2$ et donc 2. Donc : $m \mid 4(p-1)! + 4 + p$

Or $m < p$. En effet : $m < p+2$, $m \nmid p$ et si l'on avait $m = p+1$, alors $m \mid (p+2)-(p+1) = 1$ ce qui est impossible.
Donc $m \mid 4(p-1)!$ Ce qui implique que : $m \mid 4 + p$

On a : $m \mid p + 4$ et $m \mid p+2$. Donc : $m \mid (p+4)-(p+2) = 2$. Or m est impair ⇒ $\boldsymbol{m = 1}$

Comparaison des deux démonstrations :

Pour le théorème d'EUCLIDE on a obtenu : pour tout entier ***n* non premier** : $\frac{(n-1)!+1}{n}$ est irréductible.
Sur les nombres premiers jumeaux on a :

Pour tout nombre **premier *p* tel que *p*+2 ne soit pas premier** : $\frac{\frac{4\left((p-1)!+1\right)}{p}+1}{p+2}$ est irréductible.

La difficulté vient du fait qu'il est beaucoup plus facile de caractériser les entiers non premiers que les nombres premiers p vérifiant $p+2$ non premier. Pire encore, pour exploiter ce résultat, il faudrait avoir une idée de la répartition des nombres premiers non jumeaux or c'est justement, à peu de chose près, ce que l'on recherche…

Conclusions

La dernière phase de ce travail aura permis de produire deux résultats ce qui est à la fois gratifiant et motivant. Aux conclusions déjà formulées, on peut ajouter les éléments suivants :

Gestion du temps

L'absence de contrainte de temps faisait partie des éléments de l'analyse a priori. Au final, les différentes échéances (tel que la préparation de la présentation de ce travail) recréent des contraintes de temps, différentes de celles qui existent lors de la résolution d'un problème en temps limité, qui agissent davantage comme un stimulant que comme un frein.

Chercher sans trouver

Même s'il est à la fois simple et donc forcément déjà connu, le fait d'avoir trouvé le résultat annoncé au début de l'étude en utilisant une authentique démarche de recherche, est extrêmement gratifiant. Il donc difficile de pouvoir conclure sur le bilan que l'on aurait pu faire de ce travail s'il n'avait pas abouti.

Formule de J.MINÁC et C.WILLANS (1995)

Parmi les résultats rencontrés dans la littérature lors de mes recherches bibliographiques sur les démonstrations du théorème d'EUCLIDE : la formule de J.MINÁC et C.WILLANS, dont la démonstration est annoncée reposant sur le théorème de WILSON et qui donne une expression explicite de la suite des nombres premiers (et qui prouve donc a fortiori leur infinité).

$$p_n = 1 + \sum_{m=1}^{2n} \left[\left[\frac{n}{1+\sum_{j=2}^{m} \left[\frac{(j-1)!+1}{j} - \left[\frac{(j-1)!}{j} \right] \right]} \right]^{\frac{1}{n}} \right]$$

Création d'exercices

Une fois rédigée, la démonstration du théorème d'EUCLIDE par le théorème de WILSON fait penser à un exercice :

> On cherche, dans cet exercice, à démontrer le résultat suivant : il existe une infinité de nombres premiers.
>
> 1) Soit n un entier non premier ; montrer que : $\frac{(n-1)!+1}{n} \in \mathbb{Q}\backslash\mathbb{N}$
> 2) Si n n'est pas premier, montrer que n et (n-1) !+1 sont premiers entre eux.
> 3) En supposant que l'ensemble des nombres premiers soit fini : construire un nombre divisible par tous les nombres premiers puis montrer qu'il est nécessairement premier avec un autre nombre strictement supérieur à 1
> 4) Conclure sur l'infinité de l'ensemble des nombres premiers.
>
> On rappelle le théorème de WILSON : p premier si et seulement si : $(p-1)! + 1 \equiv 0\ [p]$.

La création d'exercices est une activité mathématique à part entière qui n'est pas mise en avant par les programmes comme moyen de formation. On peut pourtant l'utiliser pour travailler et comprendre des techniques (résolution de systèmes linéaires de deux équations à deux inconnues, développement et factorisation de trinômes du second degré, recherche de lieux géométriques…) ou, comme ce travail pourrait l'illustrer, avoir une activité de réflexion.

Les enseignements scientifiques fondés sur l'investigation (ESFI)

L'activité menée lors de ce travail peut se comparer à celle d'un stage Hippocampe ou d'un atelier Maths en Jeans pour des élèves : c'est-à-dire à des dispositifs qui ne font pas partie de l'organisation ordinaire de la classe.
Les ESFI (travail par tâches complexe, démarche d'investigation, narration de recherche, situation de recherche pour la classe…) valorisent, eux, le travail de recherche (même quand il n'aboutit pas) sans pour autant se placer dans une situation analogue à celle que nous venons d'expérimenter : les problèmes posés en ESFI ayant une solution (solution mathématique ou solution attendue par le professeur) le processus d'autocontrôle du travail peut jouer son rôle auprès des élèves.

Le deuxième problème des ESFI est lié à leur difficulté à mettre en œuvre des progressions réussissant à traiter tout le programme d'une classe ; le troisième problème, lié au précédent, tient à leur manque d'efficacité dans l'introduction de notions totalement nouvelles, les élèves utilisant dans leurs recherches des objets déjà connus.

La réponse institutionnelle à ces deux derniers problèmes réside dans l'utilisation d'une progression en spirale :

- Elle permet d'ouvrir tous les champs du programme très tôt dans l'année scolaire et donc d'éviter que certains sujets ne soient pas abordés.
- Chaque séance part des connaissances des élèves dans un domaine, dans le but de les approfondir et les enrichir.

La première phase de recherche effectuée pour ce travail m'a donné l'idée d'un nouveau dispositif d'ESFI :

- La classe choisit un ou des problèmes ouverts en début d'année. (projet commun, d'équipe ou individuel).
- Les élèves ont à mener une activité de recherche sur le problème qui leur est dévolu.
- L'enseignant organise et encadre ce travail de recherche.
- L'enseignant introduit à un rythme qu'il choisit, de nouvelles notions ou de nouveaux objets mathématiques qui sont testés et mis en œuvre par les élèves sur leurs problèmes de recherche.

Ce dernier point permettant de résoudre la difficulté existante entre les ESFI et l'avancée du programme de mathématiques.
Un tel enseignement ne peut s'envisager que dans le cadre d'une pédagogie de projet (contrairement aux autres ESFI) et serrait donc amené subir les contraintes inhérentes à ce type de pédagogie.

Formation initiale et continue des enseignants

La nature du travail effectué pour l'UE 34 ne ressemble à rien que je n'ai pu faire auparavant : à aucun moment dans ma formation scolaire, universitaire puis professionnelle, je n'ai eu l'occasion de me mettre en situation de recherche en mathématiques.

En maîtrise (Master 1), on réalise un TER (travail d'étude et de recherche) encadré par un enseignant chercheur ; il s'agit d'un travail d'initiation à la recherche, mais l'activité réalisé pendant le TER est beaucoup plus proche du travail fait ici sur la preuve du théorème de CLEMENT que de celui fait lors de la construction de la preuve du théorème d'EUCLIDE à partir du théorème de WILSON qui n'a pas été une initiation à la recherche, mais une mise en situation de recherche.

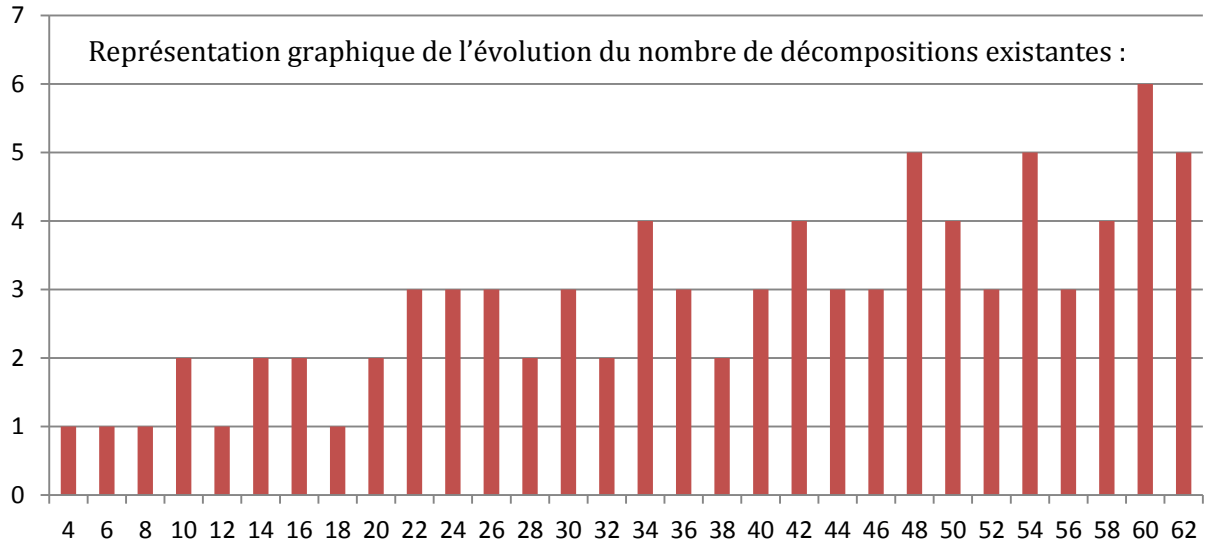
Pourtant, le fait d'avoir mené cette étude, va me conduire à repenser ma façon d'enseigner et à porter un regard différent sur les ESFI.

On peut donc se demander si des activités de mise en situation de recherche ne devraient pas être incontournables dans la formation professionnelle (initiale et continue) des enseignants et, au-delà, dans la formation universitaire des étudiants en sciences.

Annexe 1 : premières recherches

Décomposition des premiers entiers pairs en sommes de nombres premiers :

4	2+2			**34**	3+31	5+29	11+23	17+17		
6	3+3			**36**	5+31	7+29	17+19			
8	3+5			**38**	7+31	19+19				
10	5+5	3+7		**40**	3+37	11+29	17+23			
12	5+7			**42**	5+37	11+31	13+29	19+23		
14	3+11	7+7		**44**	3+41	7+37	13+31			
16	3+13	5+11		**46**	5+41	17+29	23+23			
18	7+11			**48**	5+43	7+41	11+37	17+31	19+29	
20	3+17	7+13		**50**	3+47	7+43	13+37	19+31		
22	3+19	5+17	11+11	**52**	5+47	11+41	23+29			
24	5+19	7+17	11+13	**54**	7+47	11+43	13+41	17+37	23+31	
26	3+23	7+19	13+13	**56**	3+53	13+43	19+37			
28	5+23	11+17		**58**	5+53	11+47	17+41	29+29		
30	7+23	11+19	13+17	**60**	7+53	13+47	17+43	19+41	23+37	29+31
32	3+29	13+19		**62**	3+59	19+43	23+37	29+31	31+31	



Conjecture : Soit $(G_n)_{n\in 2\mathbb{N}}$ la suite du nombre de décompositions de GOLDBACH de n : limsup$(G_n) = +\infty$ et limsup$(G_n)>1$

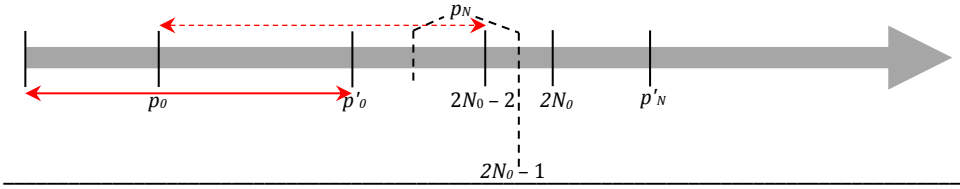
Raisonnement par l'absurde :

Soit ***M*** l'ensemble des entiers pairs non décomposables en somme de deux nombres premiers. On suppose que ***M*** est non vide ⇒ il existe un plus petit entier N_0 tel que : $\nexists\ (p\ ;p') \in \mathbb{P}^2 : 2N_0 = p + p'$. donc : $\forall\ (p\ ;p') \in \mathbb{P}^2 : 2N_0 \neq p + p'$

On peut aussi définir :

- Un couple $(p_0\ ;p_0') \in \mathbb{P}^2 : p_0 + p_0' = 2N_0 - 2$
- Le couple $(p_N\ ;p_N') \in \mathbb{P}^2 : p_N < 2N_0 < p_N'$

On a : $p_N' > p_0 + p_0'$ et : $p_N \leq 2N_0 - 1$. On aussi p_0 et $p_0' < 2N_0 - 1$. Donc $p_N > p_0$ et p_0'



Idée : regarder si un changement de base d'écriture des nombres permet de faire émerger des résultats ; on se contente de travailler sur des exemples à partir des plus petits des entiers pairs.

1. Écrire les nombres pairs dans les bases des nombres premiers présents dans leur décomposition de GOLBACH :

Entiers pairs	**Base 2**	**Base 3**	**Base 5**	**Base 7**	**Base 11**	**Base 13**	**Base 17**	**Base 19**
4	100							
6		20						
8		22	13					
10		101	20	13				
12		110	22					
14		112		20	13			
16		121	31	15	13			
18				24	17			
20		202		26		17	13	
22		211	42		20		15	13
24			44	33	22	1B	17	15

2. Écrire les nombres pairs ayant plus d'une décomposition de GOLDBACH dans la base correspondant à leur nombre de décompositions :

Entiers pairs	**Base**	**Écriture**
10	2	1010
14	2	1110
16	2	10000
20	2	10100
22	3	211
24	3	220
26	3	222
28	2	11100
30	3	1010
32	2	100000
34	4	202

Entiers pairs	**Base**	**Écriture**
36	3	1100
38	2	100110
40	3	1111
42	4	222
44	3	1122
46	3	1201
48	5	143
50	4	302
52	3	1221
54	5	204
56	3	2002
58	4	322
60	6	140
62	5	222

Propriété : $\forall\, n > 2\ \exists\, N \in 2\mathbb{N} : N =_n 222$

Démo : Soit $\boldsymbol{n}$ un entier : le nombre $\boldsymbol{N} = 2 + 2n + 2n^2$ est toujours défini et pair.

Conjecture : Pour tout $n > 2$: $N =_n 222$ possède n décompositions de GOLDBACH.

Vrai pour 26 ; 42 et 62.

En base 6 : $N = 6 + 12 + 72 = 90$

Or : $90 = 83 + 7 = 79 + 11 = 73 + 17 = 71 + 19 = 67 + 23 = 61 + 29 = 59 + 31 = 53 + 37$

Donc $G_{90} = 8 > 6$: la conjecture est réfutée.

Nouvelle conjecture : Pour tout $n > 2$: $N =_n 222$ possède au moins n décompositions de GOLDBACH.

Commentaire : la démonstration de cette conjecture permettrait la démonstration du résultat énoncé précédemment :

$$\text{limsup}(G_n) = +\infty$$

Annexe 2 : Quelques preuves classiques du théorème d'Euclide sur l'infinité des nombres premiers

Dans toutes ces démonstrations, on utilise systématiquement un autre résultat dû à EUCLIDE : tout nombre entier supérieur ou égal à 2, est décomposable, de façon unique, en produit de facteurs premiers.

EUCLIDE : preuve historique :

Soit $\{p_1 ; p_2 ; \ldots\ldots p_n\}$ une liste de nombre premiers.

Aucun de ces nombres ne divise p_n !+1. Il existe donc un nombre premier ***p*** qui n'appartient pas à cette liste.

Cette preuve s'appuie sur la notion d'infini potentiel.

Une preuve par l'absurde :

Supposons qu'il existe un nombre fini de nombres premiers. Soit p_M le plus grand des nombres premiers :

p_M !+1 > p_M n'est divisible par aucun nombre premier

⇒ **Contradiction** : il y a une infinité de nombres premiers.

Cette preuve utilise sensiblement les mêmes arguments que la précédente, mais elle s'appuie sur la notion d'infini actuel.

Une preuve faisant intervenir les nombres de FERMAT :

Le (n+1)ème nombre de FERMAT s'écrit : $F_n = 2^{2^n} + 1$. Montrons que deux nombres de FERMAT distincts sont toujours premiers entre eux :

Propriété : $\prod_{k=0}^{n-1} F_k = F_n - 2 \;.\forall\; n \geq 1$

Démonstration par récurrence sur *n* :

- $n = 1 : \prod_{k=0}^{0} F_k = F_0 = 3$ et $F_1 - 2 = 5 - 2 = 3$.
- Au rang *n*+1 : $\prod_{k=0}^{n} F_k = F_n \times \prod_{k=0}^{n-1} F_k = (2^{2^n} + 1) \times (F_n - 2) = (2^{2^n} + 1) \times (2^{2^n} - 1) = (2^{2^n})^2 - 1^2$
  $= 2^{2^{n+1}} - 1 = F_{n+1} - 2$

Soit *j*, *i* et *m* trois entiers tels que : $i < j$ et $m \mid F_i$ et $m \mid F_j$. : $m \mid F_i$ et $i <$ j⇒ $m \mid \prod_{k=0}^{j-1} F_k$. En utilisant la propriété démontrée, ceci implique que : $m \mid F_j - 2$. Or $m \mid F_j$. donc $m \mid 2$. Comme par construction, tous les nombres de FERMAT sont impairs, *m* est égal à 1.

On a une suite de nombres entiers tous premiers entre eux deux à deux ; cela implique qu'il y a une infinité de nombre premiers (au moins un nombre premier spécifique associé à chaque nombre de FERMAT).

Hillel FURSTENBERG : une preuve topologique

On définit les ensembles d'entiers suivants : $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$; a ; $b \in \mathbb{Z}$ et $b > 0$

On définit sur $\mathbb{Z}$ la topologie suivante : O est un ouvert de $\mathbb{Z}$ si : $O = \emptyset$ ou $\forall\, a \in O\ \exists b > 0 : N_{a,b} \subseteq O$
La famille définie est bien stable par réunion et intersection finie.
On a les propriétés suivantes :

- Un ouvert non vide a un nombre infini d'éléments.
- $N_{a,b}$ est un ouvert.
- $N_{a,b}$ est un fermé en tant que complémentaire dans $\mathbb{Z}$ d'une réunion d'ouvert : $N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i;b}$

Soit p un nombre premier : $N_{0;p}$ est l'ensemble des entiers relatifs divisibles par p. Donc pour tout n dans $\mathbb{Z}$ différent de 1 ou -1, il existe au moins un p premier tel que : $n \in N_{0;p}$.

$$\text{Donc : } \mathbb{Z} \setminus \{1; -1\} = \bigcup_{p\in\mathbb{P}} N_{0;p}$$

Si l'ensemble des nombres premiers était fini, alors $\bigcup_{p\in\mathbb{P}} N_{0;p}$ serait une réunion finie de fermé de $\mathbb{Z}$, ce serait donc un fermé de $\mathbb{Z}$ et {-1 ;1} serait le complémentaire d'un fermé, c'est-à-dire un ouvert. Or les ouverts non vide de $\mathbb{Z}$ ont une infinité d'éléments : ⇒ Il ne peut pas y avoir un nombre fini de nombres premiers.

Un argument d'EULER, une preuve d'ERDŐS : L'idée : montrer que la série $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverge.

$\mathbb{P}$ est l'ensemble des nombres premiers ordonnés et numérotés : $(p_k)_{k\in\mathbb{N}^*}$

Par l'absurde : supposons que $\sum_{p\in\mathbb{P}} \frac{1}{p}$ converge : $\exists n : \sum_{\substack{p\in\mathbb{P} \\ p>p_n}} \frac{1}{p} \leq \frac{1}{2}$ (majoration du reste d'une série convergente).

Soit $N \in \mathbb{N}$; on sépare l'ensemble $\{1;....;N\}$ en deux parties disjointes :
A : ensemble des nombres divisibles par au moins un p_{n+i} avec $i>0$
B : le complémentaire de A dans $\{1;....;N\}$

$$\{1;....;N\} := A \cup B$$

Estimation du cardinal de A : chaque p_{n+i} divise au plus $\frac{N}{p_{n+i}}$ élément de $\{1;....;N\}$.

Donc $\text{card}(A) \leq \frac{N}{p_{n+1}} + \frac{N}{p_{n+2}} + \text{------} \leq N \times \sum_{k>n} \frac{1}{pk} \leq \frac{N}{2}$ et par symétrie : $\text{card}(B) \geq \frac{N}{2}$.

Soit r un élément de B. On écrit r sous la forme : : $r = m^2 q$ avec q sans facteur carré dans sa décomposition en produit de nombres premiers ; r est dans B donc q aussi, donc q ne peut compter dans sa décomposition en facteurs premiers que les nombres p_1 ; p_2 ; …… ; p_n. et chacun de ces nombres apparaît ou pas dans la décomposition de q : c'est-à-dire est à la puissance 1 ou 0 : $q = \prod_{i=1}^{n} q^{a_i}$ avec $a_i = 1$ ou 0. Il y a donc 2^n valeurs possibles pour q.

D'autre part, $m^2 \leq r$ donc : $m \leq \sqrt{r} \leq \sqrt{N}$. On a donc l'encadrement suivant : $\frac{N}{2} \leq \text{card}(B) \leq 2^n \times \sqrt{N}$

Or n est fixé par le choix de la majoration du reste de la série $\sum_{p\in\mathbb{P}} \frac{1}{p}$ par $\frac{1}{2}$ mais N lui, a été choisi arbitrairement.

Le raisonnement fait conduit donc au résultat suivant : $\forall N \in \mathbb{N} : \frac{N}{2} \leq C \times \sqrt{N}$ avec C une constante strictement positive fixée. Ceci constitue la contradiction
(on peut choisir un argument graphique ou rappeler que $\lim_{+\infty} \frac{C}{\sqrt{N}} = 0 < \frac{1}{2}$)

Annexe 3 : l'infini en mathématiques

L'infini chez les mathématiciens grecs :

Dans les textes d'EUCLIDE, la droite n'existe jamais « en entier » ; il y a seulement des segments de droites « prolongeables à volonté ».
L'infini est donc une abstraction de caractère « négatif » : l'ensemble des nombres entiers n'est jamais épuisé, l'extrémité d'une droite n'est jamais atteinte. Aucun infini n'est disponible dans sa totalité : il ne peut pas y avoir d'*infini actuel* ; l'infini est simplement envisagé comme une possibilité : on parle alors d'*infini potentiel*.
Le paradoxe de ZÉNON sur la flèche qui ne peut atteindre son but car il lui faut, à chaque instant, parcourir « la moitié du chemin qui lui reste à parcourir » avant d'arriver à la cible, peut être interprété comme une réfutation de la possibilité de l'existence de l'*infini actuel*.
Pour les grecs, la totalité des nombres entiers ne peut pas être nommée car ils admettent le principe de base : « le tout est plus grand que la partie », principe contredit par les totalités infinies. De même, le nombre $\sqrt{2}$ ne peut être nommé et n'a pas le statut d'un nombre parce qu'il ne possède pas de description arithmétique finie.
Pour contourner cette difficulté conceptuelle, EUCLIDE utilise une théorie de la comparaison des grandeurs, empruntée à EUDOXE, qui lui permet de parler des nombres réels sans jamais les nommer comme infinis actuels :

Si A et B sont deux grandeurs de même nature (par exemple des longueurs de segments) et C et D sont deux autres grandeurs de même nature (par exemple des aires de surfaces) on dira que A est à B comme C est à D lorsque, pour tout couple $(m\ ;n)$ d'entiers on a :

$$mA > nB \Rightarrow mC > nD$$
$$mA = nB \Rightarrow mC = nD$$
$$mA < nB \Rightarrow mC < nD$$

Les infinitésimaux :

La méthode des infinitésimaux développée au XVII^{ème} et XVIII^{ème} siècles pour le calcul différentiel prépare le terrain pour la reconnaissance d'un statut « ordinaire » accordé à l'infini. En raisonnant sur des infiniment grands et des infiniment petits comme si c'était des quantités finies, les mathématiciens de l'époque obtiennent des résultats auparavant inaccessibles. Les notions de nombre réel et de fonction s'avèrent alors fondamentales. Cependant, il n'y a pas dans les travaux du moment de justification convaincante pour ces objets qui ont davantage un statut d'*infinis en acte*. Il faudra attendre les années 1960 et l'analyse non standard d'Abraham ROBINSON pour voir se développer une formalisation rigoureuse du concept d'infinitésimal ; entre temps, les infinitésimaux auront été chassés du monde des mathématiques au profit de la notion de limite.

CANTOR et l'avènement l'infini actuel :

Les réflexions de CANTOR sur l'infini le mène à refonder les mathématiques sur une théorie des ensembles plutôt que sur l'arithmétique ; il considère les ensembles comme des objets ayant « une existence en soi indépendamment de nos moyen de l'atteindre » et seulement définis par leur contenu. Il introduit l'ensemble $\mathbb{N}$ des entiers naturels (pris dans leur totalité) ainsi que $\mathbb{Q}$ et $\mathbb{R}$.

Notre rapport à l'infini dans l'enseignement contemporain :

Aujourd'hui c'est plutôt la notion d'*infini actuel* qui paraît être naturelle (ou, au moins, familière). Les ensembles de nombres sont introduits assez tôt dans la scolarité et les notions de limite et de continuité sont considérées comme intuitives.

La notion d'infini potentiel va, elle, être approchée lors de l'introduction du raisonnement par récurrence, puis revisitée au début de l'enseignement supérieur à travers les espaces vectoriels de dimension infini (dont les vecteurs ont un nombre fini mais arbitrairement grand de composantes) ou les fonctions C^∞, que l'on peut dériver « autant de fois que l'on veut » sans pour autant définir une « dérivée infiniième ».

Annexe 4 : recherches de la deuxième approche

Théorème d'EUCLIDE, première piste : partir de l'étude des solutions d'une équation.

On suppose $\mathbb{P}$ fini, on définit p_0 le plus grand des nombres premiers et $\mathbb{N}_M$ l'ensemble des entiers strictement supérieurs à p_0 .

On s'intéresse aux solutions entières de la famille d'équations d'inconnue k et de paramètre n :

$$\boldsymbol{kn^2 - n - n\,! = 0}$$

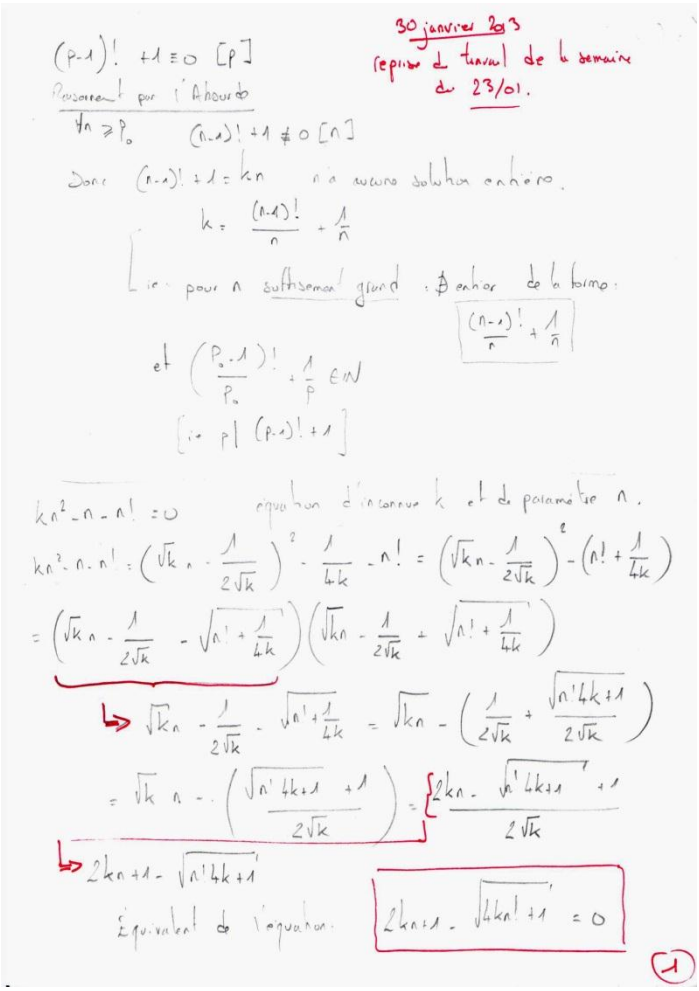
On a :

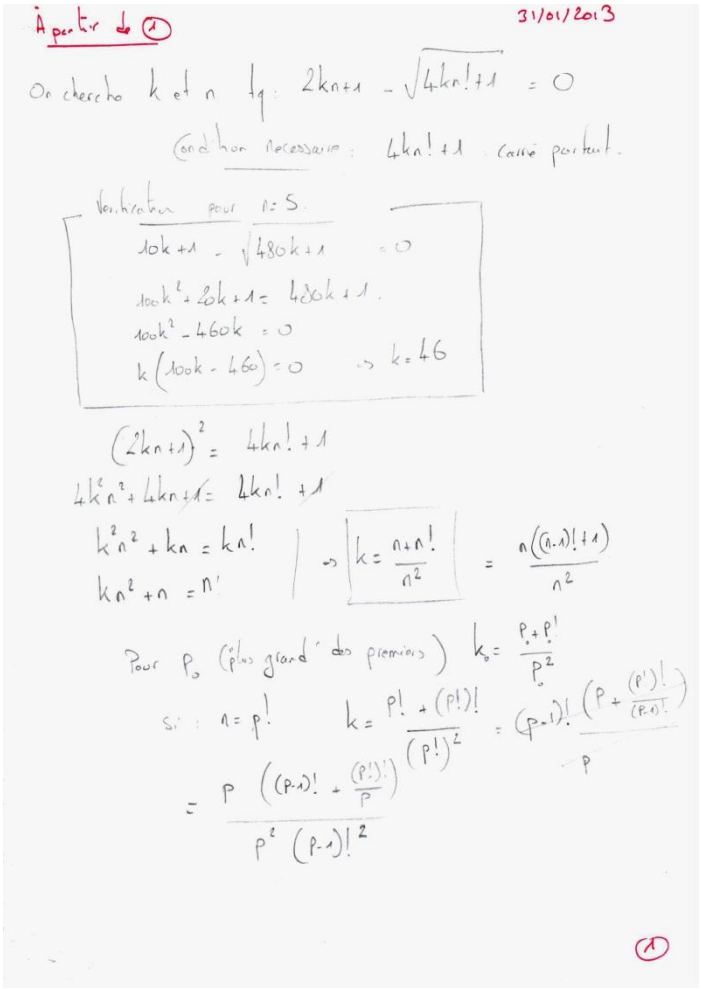
$$kn^2 - n - n\,! = (\sqrt{k}n - \frac{1}{2\sqrt{k}})^2 - \frac{1}{4k} - n! = (\sqrt{k}n - \frac{1}{2\sqrt{k}})^2 - (n! + \frac{1}{4k}) = \left(\sqrt{k}n - \frac{1}{2\sqrt{k}} - \sqrt{n! + \frac{1}{4k}}\right)\left(\sqrt{k}n + \frac{1}{2\sqrt{k}} - \sqrt{n! + \frac{1}{4k}}\right)$$

Et : $\sqrt{k}n - \frac{1}{2\sqrt{k}} - \sqrt{n! + \frac{1}{4k}} = \sqrt{k}n - \left(\frac{1}{2\sqrt{k}} + \sqrt{n! + \frac{1}{4k}}\right) = \sqrt{k}n - \frac{\sqrt{n!4k+1}+1}{2\sqrt{k}} = \frac{2kn - \sqrt{n!4k+1}+1}{2\sqrt{k}}$

Notre équation est donc équivalente à : $2kn + 1 - \sqrt{n!\,4k+1} = 0$

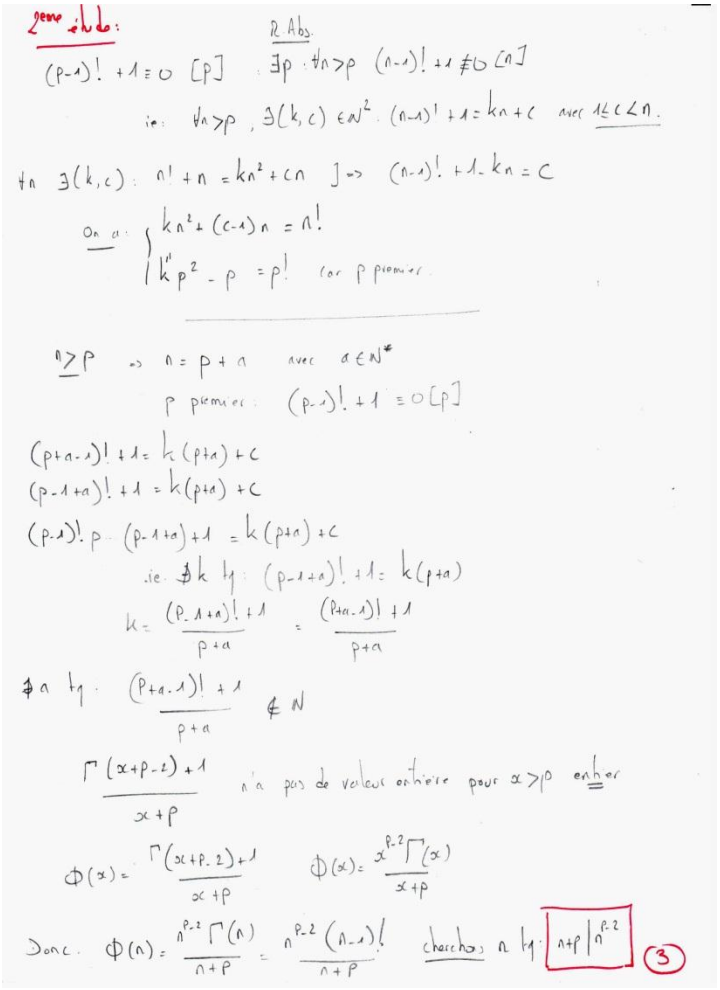
Condition nécessaire : n !$4k$+1 est un carré parfait.

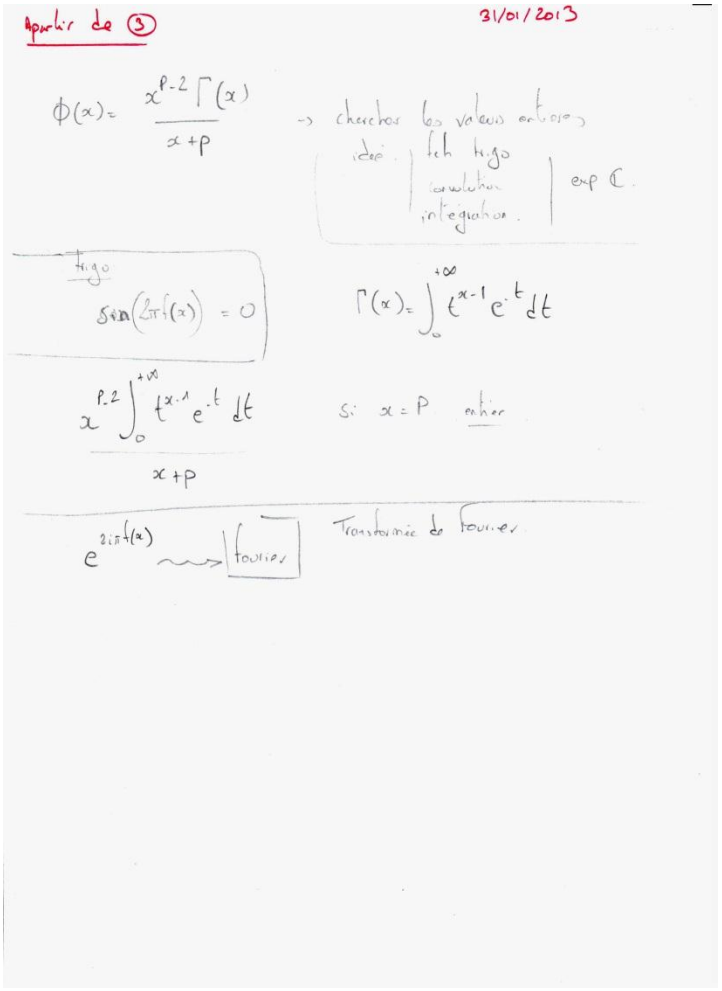




Théorème d'EUCLIDE, deuxième piste : partir de l'étude d'une fonction.

On va introduire la fonction $\Phi(x)$de $\mathbb{N}$ dans $\mathbb{Q}$ définie par :$\Phi(x) = \frac{x^{p-2}}{x+p}\Gamma(x)$





À partir de là, il faudrait être capable de construire un outil ou une méthode permettant d'identifier les valeurs entières d'une fonction. On pense naturellement à l'emploi de fonctions circulaires.

Caractérisation des nombres premiers jumeaux grâce au théorème de WILSON :

p et $p + 2$ premiers jumeaux :

$$(p - 1) ! + 1 \equiv 0\ [p]$$

$$(p + 1) ! + 1 \equiv 0\ [p + 2]$$

$(p - 1) ! + (p + 1) ! + 2 = kp + k'p + 2k'$

$(p + 1) ! = (p - 1) !p(p + 1)$ donc $(p - 1) ! + (p + 1) ! = (p - 1) !(1 + p(p + 1))$

$(p - 1) ! - (p + 1) ! = k'(p + 2) - kp = (p - 1) !(p^2 + p - 1)$

Or : $(p + 1) ! + 1 \equiv 0\ [p + 2] \Rightarrow (p + 1) ! + 1 = kp + 2k$ et donc : $(p + 1) ! + 1 \equiv 2k\ [p]$

Donc : $\boxed{(p - 1) !(p^2 + p - 1) \equiv 2k\ [p] \quad \text{soit :} \quad \frac{(p-1)!}{2}(p(p+1) - 1) \equiv k\ [\frac{p}{2}]}$

Annexe 5 : Independence des théorèmes d'EUCLIDE et de WILSON

Théorème de WILSON : ***p* premier si et seulement si : (*p* -1)! + 1 ≡ 0 [*p*]**

Condition nécessaire :

Pour $p = 2$ et $p = 3$ on vérifie que : $1 !+1 = 2 \equiv 0$ [2] et $2 !+1 = 3$ $x - \overline{1})(x + \overline{1}$ [3]

Soit $p > 3$ un nombre premier. : **$\mathbb{Z}/p\mathbb{Z}$ est un corps**. Soit $(\mathbb{Z}/p\mathbb{Z})^*$ son groupe multiplicatif ; on cherche les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ égaux à leur inverse :
$x \in (\mathbb{Z}/p\mathbb{Z})^*$ et $x = x^{-1} : x\,x^{-1} = \overline{1} = x\,x = x^2$. Donc : $x^2 .- \overline{1} = \overline{0} \Leftrightarrow (x - \overline{1})(x + \overline{1}) = \overline{0} \Leftrightarrow x = \overline{1}$ ou $x = - \overline{1} \equiv p - 1$ [p]

Donc en regroupant $\overline{2}; \overline{3}; \ldots . \overline{p-2}$ en $\frac{p-3}{2}$ paires $\{x_i ; y_i\}$ telles que : $x_i = y_i^{-1}$ on obtient :

$\overline{2}\,\overline{3} \ldots . \overline{p-2} = \prod_{i=1}^{\frac{p-3}{2}} (x_i y_i) = \overline{1}$ et donc : $(\overline{p-1})\,! = \overline{1} \prod_{i=1}^{\frac{p-3}{2}} (x_i y_i)\ \overline{(p-1)} = \overline{(1)(1)(-1)} = \overline{-1}$ d'où : $(p\text{ -1})! \equiv -1$ [p]

Condition suffisante :

Soit n un entier supérieur à 1 vérifiant : $(n\text{ -1})! + 1 \equiv 0$ [n]. Soit a un diviseur de n strictement inférieur à n.
On a : $a \mid (n\text{ -1})! + 1$ et comme $a \leq (n - 1)$ on a aussi : $a \mid (n\text{ -1})! \Rightarrow a \mid 1 \Rightarrow a = 1$:

$n > 1$ n'est divisible que par 1 et n : n est premier.

p premier ⇒ $\mathbb{Z}/p\mathbb{Z}$ est un corps :

Pour $n \in \mathbb{N}$: $(\mathbb{Z}/n\mathbb{Z} ; + ; \times)$ est un anneau. Montrons que si p est premier, alors tout élément de $(\mathbb{Z}/p\mathbb{Z})^*$ est inversible :
Pour tout entier n tel que : $1 \leq n \leq p - 1$ on a : $n \wedge p = 1$. En appliquant le **théorème de BACHET – BÉZOUT** on obtient :
$\exists\, (u ; v) \in \mathbb{Z}^2 : un + vp = 1$ et donc : $\exists\, u \in \mathbb{Z} : \bar{u}\bar{n} = \overline{1}$ [p]. Tout élément de $(\mathbb{Z}/p\mathbb{Z})^*$ est inversible.

Théorème de BACHET – BÉZOUT : Étude de la démonstration de [$a \wedge b = 1$] ⇒ [$\exists\, (u ; v) \in \mathbb{Z}^2 : ua + vb = 1$]

Soit $(a ; b) \in \mathbb{Z}^2 : a \wedge b = 1$.(En particulier : $ab \neq 0$). On pose : $U = \{xa + yb\ ;\ (x ; y) \in \mathbb{Z}^2\}$. : $|a| \in U$ donc $U \cap \mathbb{N}^* \neq \emptyset$.
Donc $U \cap \mathbb{N}^*$ possède un plus petit élément : $d_0 = x_0\, a + y_0\, b$. Si on effectue la division euclidienne de a par d_0 on obtient : $a = qd_0 + r$. et $r = a - qd_0 = a - q(x_0\, a + y_0\, b) = a - qx_0\, a - qy_0\, b .= (1 - qx_0)a + (- qy_0)b$ donc $r \in U$ et $r \geq 0$

On a : $0 \leq r < d_0$ donc $r \notin U \cap \mathbb{N}^*$ mais $r \in U$ et $r \geq 0 \Rightarrow r = 0$. Cela signifie que d_0 divise a et faisait un raisonnement symétrique utilisant b , on en déduit que d_0 divise aussi b : d_0 est un diviseur commun de a et $b \Rightarrow d_0 = 1$.

Et donc : $\exists\, (x_0; y_0) \in \mathbb{Z}^2 : x_0 a + y_0 b = 1$

À aucun moment on a utilisé le fait qu'il y a une infinité de nombres premiers.

Annexe 6 : Théorème de CLEMENT

Article original : P.A. CLEMENT Janvier 1949 :

CONGRUENCES FOR SETS OF PRIMES

P. A. CLEMENT, University of California, Los Angeles

1. Introduction. Wilson's function $P_1(n)$ is the function $P_1(n) \equiv (n-1)!+1$. By Wilson's theorem the condition $P_1(n) \equiv 0 \bmod n$ is necessary and sufficient in order that an integer $n>1$ be prime. In this note we find a congruence condition, similar to the above, for twin primality, and we indicate a method which furnishes a condition for sets of prime numbers of any prescribed type.

2. Twin primes. We shall establish the following result:

THEOREM. *A necessary and sufficient condition that two integers, n and $n+2$, $n>1$, both be prime is that*

$$4[(n-1)!+1]+n \equiv 0 \bmod n(n+2). \tag{1}$$

Proof. The sufficiency is obvious as divisions by n and $n+2$ separately reduce either to Wilson's theorem or to a simple modification of it.

The necessity follows as easily, but we wish to indicate how (1) may be obtain directly. Thus, with n and $n+2$ both primes, we have

$$(n-1)!+1 \equiv 0 \bmod n, \tag{2}$$

$$(n+1)!+1 \equiv 0 \bmod (n+2). \tag{3}$$

Reducing the factorial of (3) mod $(n+2)$ and rewriting as an equation we obtain

$$2[(n-1)!]+1 = k(n+2), \qquad k \text{ some integer;} \tag{4}$$

then, using (2), we must have

$$2k+1 \equiv 0 \bmod n. \tag{5}$$

Substitution of (5) in (4) determines the congruence of the theorem.

It may be noted that if 1 is considered the first prime, then the restriction $n>1$ can be deleted from the above theorem.

Étude de la preuve :

Condition nécessaire et suffisante pour que deux entiers p et p+2 soient tous les deux premiers:

$$\mathbf{4((\,p-1)!+1)+p\equiv 0\ [\,p\,(p+2)]}$$

Condition suffisante :

Soit $\boldsymbol{p}$ un entier tel que $\boldsymbol{p}$ et $\boldsymbol{p}$ +2 soient premiers :
Théorème de WILSON : $(p+1)!+1\equiv 0\ [p+2] \Leftrightarrow p(p+1)(p-1)!+1\equiv 0\ [p+2]$
On a : $p(p+1)=p^2+p\equiv p^2+p+(p+2)\ [p+2]\equiv p\,(p+1+1)+2\ [p+2]\equiv 2\ [p+2]$

Donc : $(p+1)!+1\equiv 0\ [p+2] \Leftrightarrow 2(p-1)!+1\equiv 0\ [p+2]$
D'où: $2(p-1)!+1=k\,(p+2)$ et: $2(p-1)!+1=\underbrace{(p-1)!+1}_{\equiv 0\,[p]}+\underbrace{(p-1)!}_{\equiv -1\,[p]}=2k+\underbrace{2p}_{\equiv 0\,[p]}$

Donc : $2k+1\equiv 0\ [p]$

On a : $4((p-1)!+1)+p=2(p-1)!+1+2(p-1)!+1+2+p=2(2(p-1)!+1)+p+2=2(k\,(p+2))+p+2$
$=\underbrace{(2k+1)}_{\equiv 0\,[p]}\underbrace{(p+2)}_{\equiv 0\,[p+2]}\equiv 0\ [p\,(p+2)]$

Condition nécessaire:

Soit $\boldsymbol{n}>1$ un entier tel : $\mathbf{4((\,n-1)!+1)+n\equiv 0\ [\,n\,(n+2)]}$

$\exists\, k\in\mathbb{N}$: $4((n-1)!+1)=k\,n\,(n+2)-n=n\,(k\,n\,(n+2)-1)$ et donc : $4((n-1)!+1)\equiv 0\ [n\,]$

$(n-1)!+1$ impair donc d'après le théorème de GAUSS : n divise 4 ou n divise $(n-1)!+1$)
Pour $n=4$ on a : $4(4-1)!+1)+4=32$ et $4(4+2)=24$. Or $24\nmid 32$;

Donc

$4((n-1)!+1)+n\equiv 0\ [n\,(n+2)] \Rightarrow n\mid (n-1)!+1) \Rightarrow n$ est premier d'après le théorème de WILSON.

Montrons maintenant que $n+2$ est également premier :

On a :$4((n-1)!+1)=k\,n\,(n+2)-n=n\,(k\,n\,(n+2)-1)$

Donc : $4(n-1)!=n\,(k\,n\,(n+2)-1)-4 \Leftrightarrow 4(n+1)!=n^2\,(n+1)(k\,(n+2)-1)-4n\,(n+1)$

$\Leftrightarrow 4((n+1)!+1)=n^2\,(n+1)(k\,(n+2)-1)-4n\,(n+1)+4$

Montrons maintenant que $n^2\,(n+1)(k\,(n+2)-1)-4n\,(n+1)+4$ est factorisable par $(n+2)$:

On introduit : $P(X)=X^2\,(X+1)(k\,(X+2)-1)-4X\,(X+1)+4$ et on calcule : $P(-2)=0$

D'où : $4((n+1)!+1)\equiv 0\ [n+2]$: d'après le théorème de WILSON : $n+2$ est premier.

On a démontré que : $\boldsymbol{p}$ **et** $\boldsymbol{p+2}$ **sont premiers** $\Leftrightarrow \mathbf{4((\,p-1)!+1)+p\equiv 0\ [\,p\,(p+2)]}$