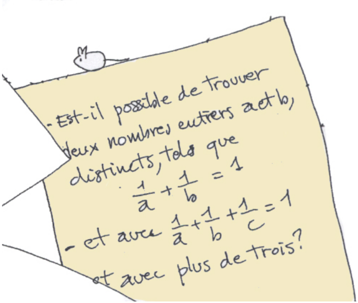

La base 60 n'a pas fini de nous étonner...

Préliminaires

Lors de la rencontre à l'INRP des 13 et 14 juin 2007, le groupe EXPRIME m'a demandé si je connaissais les nombres parfaits ; c'était en lien avec la décomposition de 1 en fractions égyptiennes.
Eh oui le premier nombre parfait, $6 = 3 + 2 + 1$ (somme de ses diviseurs propres) permet de trouver, en divisant par 6, $1 = \dfrac{1}{2} + \dfrac{1}{3} + \dfrac{1}{6}$; le deuxième parfait $28 = 1 + 2 + 4 + 7 + 14$ permet de trouver $1 = \dfrac{1}{28} + \dfrac{1}{14} + \dfrac{1}{7} + \dfrac{1}{4} + \dfrac{1}{2}$.

Retour aux Situations Connexes
Suite

Le soir je cherche les parfaits suivants, ce sont 496 puis 8128 ; le suivant est très très grand car quelques algorithmes plus tard et une heure plus tard je suis sûr qu'il a plus de 8 chiffres (en base 10). Mais il est évident que chaque nombre parfait nous donne immédiatement une décomposition de 1 en fractions égyptiennes.

J'interroge la base de données sur les suites : ▸ Voir le site ; elle me donne les résultats suivants : 33550336, 8589869056, 137438691328, 2305843008139952128, 2658455991569831744654692615953842176, 191561942608236107294793378084303638130997321548169216 et de nombreuses références, propriétés et conjectures sur les nombres parfaits. En fait il faut souligner ici que cette base de données est un outil incontournable pour qui veut saisir ce que les ordinateurs et le « ouaibe » ont amené aux mathématiques à un niveau de l'expérimental : en clair par essais, vérifications, conjectures, ... on connaît le début d'une suite ; le réflexe approprié est alors de consulter cette base de données, chose qui n'était pas possible au siècle dernier.
Oui l'expérimental s'accompagne toujours de « savoir-faire » ; ici je souligne l'importance de ce nouveau savoir-faire, récent. Jusqu'à très peu, en mathématique, les « savoir-faire » étaient associées à des techniques de preuves, des heuristiques, également à des recherches de savoirs et bibliographiques, etc. ; maintenant il faut « savoir » utiliser de nouveaux outils : c'est un « savoir-faire », autant nouveau qu'indispensable, qui colore l'expérimental en mathématique.

◂ Retour aux Situations Connexes ▸ Suite

1. Et les abondants ?

Le lendemain matin, armé des résultats trouvés, j'annonce aux collègues, heureux du travail accompli, mais déçu par le résultat, « les nombres parfaits, c'est une bonne idée concernant la génération de 1 en somme de fractions égyptiennes, mais malheureusement ils sont rares, cela ne peut guère générer le foisonnement de décompositions en fractions égyptiennes de l'unité. Et puis on sait que le nombre de décompositions de $\frac{1}{n} = \frac{1}{a} + \frac{1}{b}$ est donné par le nombre de diviseurs de n^2 plus petit que n, autrement dit si on savait classifier explicitement toutes les décompositions de 1 en fractions égyptiennes, on aurait résolu le problème de décomposition d'un nombre en produit de facteurs premiers ! Il ne faut pas rêver ».
Mais ils sont têtus les copains, 3 heures après, « Eh, au lieu de prendre un nombre parfait, si on prend un nombre abondant, alors on peut écrire 1 comme somme de fractions égyptiennes ». Il fallait y penser, merci les braves.
Toujours est-il que mon ordinateur a chauffé deux soirées ; en voici le produit : quelques résultats numériques puis un théorème (ce qui veut dire que le recours au papier et crayon pour écrire une preuve termine toujours un épisode expérimental fructueux) et enfin un questionnement sur les nombres « très abondants », comme 60 et 120, alimente ma réflexion sur les nombres.
Cependant, il ne faut toujours pas rêver, pas d'algorithme n'en sortira pour décomposer rapidement un nombre en ses facteurs premiers, donc pas de casse prévisible de codification de messages par une méthode du type « RSA ».

1.1 Sur les nombres abondants

Définition et notations : Un entier N est abondant si la somme de ses diviseurs propres est plus grande que N ; dans la suite nous dirons qu'un nombre est abondant (au sens large) s'il est abondant au sens strict ou s'il est parfait. Nous noterons $\mathcal{S}$ l'ensemble des diviseurs propres s de N et $S(N)$ la somme de ces diviseurs propres.
Voici les premiers nombres abondants (ou parfaits) :
6, 12, 18, 20, 24, 28, 30, 36, 40, 42, 48, 54, 56, 60, 66, 70, 72, 78, 80, 84, 88, 90, 96, 100,102, 104, 108, 112, 114, 120, ...
Attention, tous les nombres abondants ne sont pas pairs ; le plus petit impair est $N = 945$, avec $S(945) = 975$.
Prenons maintenant une décomposition de l'unité en somme de fractions égyptiennes distinctes (FE) : $1 = \frac{1}{n_1} + \frac{1}{n_2} + ... + \frac{1}{n_k}$, avec : $1 < n_1 < n_2 < \ ... \ < n_k$.
On a le résultat suivant (immédiat à démontrer, mais remarqué qu'après un certain nombre de manipulations) :

Lemme : soit une FE (décomposition de 1 en fractions égyptiennes distinctes), alors $N = ppcm(n_1,\ n_2,\ \ ...\ ,\ n_k)$ est abondant (au sens large).

Retour aux Situations Connexes   Suite

Pour la preuve, il suffit de multiplier par N l'équation (FE) : $N = \frac{N}{n_1} + \frac{N}{n_2} + \ldots + \frac{N}{n_k}$ et de remarquer que les fractions $\frac{N}{n_i}$ sont des entiers distincts diviseurs de N, et donc $S(N) \geq N$.

Moralité : à toute décomposition de 1 en FE, on associe canoniquement un nombre abondant.

Questionnement : inversement, prenons un nombre abondant N, comment et combien de décompositions de 1 en FE peut-on obtenir ?
Autrement dit, soit N un abondant alors il faut résoudre l'équation :

$$N = \sum \epsilon_i \, s_i$$

pour $s_i \in \mathcal{S}$ et $\epsilon_i \in \{0, 1\}$.
Pour toute solution de cette équation on obtient une décomposition de 1 en FE. En particulier il est évident que pour tout nombre parfait on obtient une et une seule solution, donc une et une seule décomposition de 1 en FE.

◂ Retour aux Situations Connexes ▸ Suite

Voici un **programme** (relativement court, mis au point après d'autres programmes plus simples), avec un logiciel de calcul formel qui permet de construire quelques solutions pour tout N, $N <= 120$: nous verrons après la difficulté liée au nombre abondant 120.

```
> with(numtheory,divisors) :
>sommes :=proc(n)
local a,b,c,A,j,k,m,v ;
a :={0} union (divisors(n) minus {n}) ;b :=nops(a) ;c :=convert(a,'+')-n ;
A :=NULL :
for j in a do if c-j in (a minus {j}) union {0} then
A :=A,map(u->u/n,a minus {c-j,j,0}) ;
elif c-j>0 then for k in a minus {j} do if c-j-k in a minus {j,k}
then A :=A,map(u->u/n,a minus {c-j-k,j,k,0}) ;
else for m in a minus {j,k} do if c-j-k-m in a minus {j,k,m}
then A :=A,map(u->u/n,a minus {c-j-k-m,j,k,m,0}) ;
fi ;od :fi ;od :
fi ;
od :
A ;
end :
```

◂ Retour aux Situations Connexes ▸ Suite

On applique cette procédure aux premiers nombres abondants, ce qui donne :
>F := [6, 12, 18, 20, 24, 28, 30, 36, 40, 42, 48, 54, 56, 60] :
>seq([F[i],sommes(F[i])],i=1....14) ;

$$6, \{\{1/2, 1/6, 1/3\}\}$$

$$12, \{\{1/2, 1/6, 1/3\}\{1/12, 1/2, 1/6, 1/4\}\}$$

$$18, \{\{1/2, 1/6, 1/3\}, \{1/2, 1/3, 1/9, 1/18\}\}$$

$$20, \{\{1/2, 1/4, 1/5, 1/20\}\}$$

$$24, \{\{1/12, 1/24, 1/8, 1/6, 1/4, 1/3\}\{1/12, 1/2, 1/6, 1/4\}, \{1/2, 1/24, 1/8, 1/3\}, \{1/12, 1/2, 1/24, 1/8, 1/4\}\}$$

$$28, \{\{1/2, 1/4, 1/7, 1/14, 1/28\}\}$$

$$30, \{\{1/2, 1/6, 1/5, 1/10, 1/30\}, \{1/2, 1/3, 1/10, 1/15\}\}$$

$$36, \{\{1/12, 1/6, 1/4, 1/3, 1/9, 1/18\}, \{1/2, 1/36, 1/6, 1/4, 1/18\},$$
$$\{1/12, 1/2, 1/36, 1/3, 1/18\}, \{1/12, 1/2, 1/4, 1/9, 1/18\}\}$$

$$40, \{\{1/2, 1/40, 1/8, 1/5, 1/20, 1/10\}, \{1/2, 1/40, 1/8, 1/4, 1/10\}, \{1/2, 1/4, 1/5, 1/20\}\}$$

$$42, \{\{1/2, 1/3, 1/42, 1/7\}\}$$

$$48, \{\{1/48, 1/24, 1/16, 1/8, 1/6, 1/4, 1/3\}, \{1/12, 1/24, 1/8, 1/6, 1/4, 1/3\},$$
$$\{1/2, 1/48, 1/24, 1/16, 1/8, 1/4\}, \{1/12, 1/2, 1/48, 1/24, 1/16, 1/8, 1/6\}\}$$

$$54, \{\{1/2, 1/3, 1/27, 1/54, 1/9\}, \{1/2, 1/3, 1/9, 1/18\}\}$$

$$56, \{\{1/2, 1/8, 1/4, 1/56, 1/14, 1/28\}, \{1/2, 1/4, 1/7, 1/14, 1/28\}\}$$

$$60, \{\{1/12, 1/6, 1/3, 1/5, 1/60, 1/10, 1/30, 1/\}, \{1/12, 1/6, 1/4, 1/3, 1/20, 1/60, 1/30, 1/15\}\}$$

◂ Retour aux Situations Connexes ▸ Suite

Ainsi à chaque abondant on peut associer une ou plusieurs décomposition de 1 en somme de FE. Mais on ne les obtient pas tous au moyen de ce programme. Quelques procédures plus tard, plus sophistiquées, longues à écrire mais plus rapides, on obtient toutes (?) les décompositions possibles de 1 en FE, pour $N < 120$. Il y en a quelques unes pour chaque abondant. (j'ai vérifié à la main pour les premiers abondants, il faut toujours se méfier des résultats donnés par un ordinateur, non pas parce qu'il se trompe, mais parce qu'on a pu mal programmer et donc il nous renvoie un résultat faux en soi, mais juste en fonction de ce qu'on lui a demandé d'accomplir). Mais pour $N = 60$, on a 33 décompositions distinctes (est-ce exact ?).
Pourquoi tant, parce qu'il y a des nombres beaucoup plus abondants que d'autres ($S(N)$ grand par rapport à N) ; c'est le cas pour 60 et 120.
Pour 120, j'en ai trouvé déjà 276. Mais je ne sais pas si je les ai toutes obtenues.
A retenir donc trois choses :

- La classification des décompositions de 1 passe par les nombres abondants.
- Cette méthode permet de trouver toutes les décompositions de 1 en FE avec des dénominateurs bornés (par un N abondant choisi a priori).
- Le seul nombre abondant qui fut utilisé historiquement comme base de numération est le nombre 60 ; et il est très abondant ($S(60) = 108$). Ceci permet-il de mieux comprendre pourquoi la méthode des fractions égyptiennes fut utilisée empiriquement en lien avec cette numération en base 60 qui permet tant de partages différents ?

Évidemment il reste des questions, par exemple pourquoi 33 et non pas 19 ou 421 décompositions pour le nombre abondant 60 ? (Écrit à Vaulx-en-Velin le 21 Juin 2007)

◂ Retour aux Situations Connexes   ▸ Suite

1.2 Sur les nombres presque-parfaits

Reprise le 23 juin, avec la mise au point d'un programme simple et rapide qui donne « la plus petite décomposition de 1 en FE » à partir d'un abondant.
Deux suites de nombres qui posent questions se font jour :

- Une suite dont les premiers termes sont 70, 836 et 4030, paramétrant des abondants qui ne donnent pas lieu à une décomposition de 1 en FE ;
- Une suite dont les premiers termes sont 6, 20, 88, 104 et 272, paramétrant des abondants qui donnent une décomposition minimale dont le « ppcm » associé redonne l'abondant de départ.

Le réflexe immédiat fut d'interroger la base de données des suites (cf. plus haut) ; on trouve les suites nommées respectivement A006037 des abondants qui ne sont pas « presque-parfaits » ▸ Visiter la page du site et A006036 des « presque-parfaits primitifs ». ▸ Visiter la page du site
Ces deux suites font référence à celle des « presque-parfaits » (A005835) qui est celle constituée des nombres ... ▸ Visiter la page du site :

Définition : Un entier est presque-parfait s'il est somme de certains de ses diviseurs distincts ;i.e. ce sont donc les nombres abondants (ou parfaits) donnant automatiquement lieu à une décomposition de 1 en FE. Autrement dit la boucle est bouclée, la connaissance des décompositions de 1 en FE est équivalente à la connaissance des nombres presque-parfaits ; il reste à expliciter cette correspondance (à ma connaissance rien dans la littérature).

◂ Retour aux Situations Connexes ▸ Suite

Par ailleurs sur la page A005835 des nombres presque-parfaits figure un programme en « maple » pour les trouver ; je l'adapte pour les décompositions de 1 en FE, de fait il n'est pas plus rapide que ceux que j'ai mis au point mais il est plus complet : il trouve 34 (au lieu de 33) décompositions de 1 en FE pour le nombre 60 et 278 (au lieu de 276) pour le nombre 120.
Voici ce programme (attention très technique et peu lisible pour un non-initié au calcul formel)) :

```
> with(numtheory,divisors) :with(combinat) :
> semiparfait :=proc(n)
local A,a,S ; S :=subsets(divisors(n) minus n) :A :=NULL :
while not S[finished] do a :=S[nextvalue]() ; if convert(a,'+')=n then A :=A,a ;
fi ; od ; return A
end :
> semiparfait(30) ;nops([semiparfait(70)]) ;nops([semiparfait(60)]) ;
5, 10, 15, 2, 3, 10, 15, 1, 3, 5, 6, 15
0
34
```

Il ne reste plus qu'à faire une synthèse sous la forme du théorème :

Théorème : A toute décomposition de 1 en somme de fractions égyptiennes, alors le ppcm des dénominateurs est un nombre presque-parfait ; inversement à tout nombre presque-parfait on associe canoniquement un ensemble de décompositions de 1 en somme de fractions égyptiennes, cet ensemble comprenant une décomposition dont le ppcm des dénominateurs est le nombre presque-parfait de départ.

2. Conclusions

- Par le théorème ci-dessus, les deux concepts de « décompositions de 1 en somme de fractions égyptiennes » et de « nombres presque-parfaits » sont non seulement reliés mais les rapports entre les deux sont explicités.
- Tout spécialiste en théorie des nombres dira, à juste titre, que le résultat (le théorème ci-dessus) est une trivialité, et il aura raison puisque les démonstrations sont à « deux sous », mais ce que ces experts oublient, c'est le fait que nous sommes partis du concept historique de fractions égyptiennes et de l'avoir situé, grâce à une approche originale, dans le cadre de la théorie des nombres. Est-ce que ce rapprochement permettra des reformulations pertinentes de certaines conjectures dans cette même théorie ? Je ne le pense pas, mais sait-on jamais !
- Si l'importance historique des fractions égyptiennes est attestée, il est intéressant de se poser la question de savoir ce que ce travail (d'un groupe) peut amener au point de vue épistémologique. De ce point de vue, il me semble qu'à travers cet exemple des fractions égyptiennes, le sens et le rôle de « l'expérimental en mathématiques » sont précisés, en tenant compte des nouvelles technologies (TICE)

J'espère que cette « narration de recherche » pourra permettre de mieux situer l'apport des TICE dans le domaine de l'expérimental en mathématiques qui a toujours été, et qui le restera toujours, le fait de s'appuyer sur des concepts naturalisés pour accéder et s'approprier de nouveaux concepts (plus abstraits) qui à leur tour seront naturalisés. *Le 25 juin 2007.*

◂ Retour aux Situations Connexes ▸ Suite

3. Deuxième partie : des résultats de l'été 2007
3.1 Contexte

Dans la semaine du 20 Août 07, il s'est déroulé l'université d'été organisée par l'inspection générale de mathématiques sur le thème : « Expérimentation et démarches d'investigation en mathématiques ». Nous sommes intervenus à deux, pour essayer de retransmettre des éléments forts de notre groupe EXPRIME. A partir du problème des fractions égyptiennes, j'ai animé un atelier de travail le mardi 21 (deux groupes entre 14h et 18h.30 sur le thème :« La dimension expérimentale au cœur des problèmes de recherches en mathématiques ») ; le lendemain matin, Gilles Aldon a donné une conférence plénière ayant pour titre « La place des TICE dans une démarche expérimentale en mathématiques ».
Au cours du mois de juillet Gilles A. avait retransmis l'essentiel de nos travaux à Budapest lors d'un colloque mondial sur un thème similaire.
Aussi, rien d'étonnant à ce que, d'une part Gilles et moi ayons préparé tout cela ensemble et tranquillement avant le 20 juillet, d'autre part que j'ai fait chauffer l'ordinateur et mes neurones à partir du 18 Août.
Ici je vais essayer de donner les liens entre fractions égyptiennes et problèmes de recherche en arithmétique aujourd'hui. Nous verrons même que le nombre 19 est derrière ces liens, pourquoi ? je ne le sais pas, mais c'est un fait.

◂ Retour aux Situations Connexes ▸ Suite

3.2 Fractions égyptiennes et nombres presque-parfaits (suite)

Un problème délicat est de trouver un algorithme simple qui nous donne les 6 décompositions de 1 en somme de quatre fractions égyptiennes, puis les 72 décompositions de 1 en somme de 5 fractions égyptiennes, etc.
Plutôt que de vous raconter les méandres de ma recherche, voici le résultat (obtenu le 19 Août) qui explicite le principe algorithmique.
Considérons la décomposition de 1 en somme de trois fractions égyptiennes ($1 = 1/2 + 1/3 + 1/6$). Prenons le ppcm, que nous noterons a, des dénominateurs (égal à 6), puis prenons les diviseurs d de a^2 plus petit que a ($d \in \{1, 2, 3, 4\}$).
Considérons alors les décompositions de 1 en somme de 4 fractions égyptiennes obtenues à partir des nombres (abondants) presque-parfaits $a(a + d)$; on retrouve les 6 décompositions cherchées. A l'étape suivante, pour les 6 ppcm a provenant des décompositions de 1 en quatre FE, ce sont les presque-parfaits 12, 18, 20, 24, 30 et 42, on trouve les 72 décompositions de 1 en somme de 5 fractions égyptiennes. Etc.
Ainsi on a un bon algorithme théorique, mais il est lent, trop lent pour pouvoir trouver les 2320 décompositions de 1 en somme de 6 fractions égyptiennes à partir des 72 ppcm associés aux décompositions de 1 en somme de 5 FE ; en effet pour chacun de ces 72 ppcm a, il faut obtenir les diviseurs d de a^2 plus petits que a puis calculer les décompositions (en somme de 6 fractions égyptiennes) associées aux presque-parfaits $a(a + d)$. Bien au niveau théorique, mauvais au niveau calculatoire. En cherchant un algorithme plus performant, j'ai glané quelques petits résultats ; en voici deux.

Retour aux Situations Connexes　Suite

Définition : On dira qu'un entier N est quasi-parfait s'il peut s'écrire de manière unique comme somme de certains de ses diviseurs stricts d_k, et si de plus N est le ppcm des nombres N/d_k. (i.e. à chaque quasi-parfait est associé une unique décomposition de 1 en FE dont le ppcm des dénominateurs est ce quasi-parfait).

Exemples : les nombres parfaits (somme de tous ses diviseurs stricts) sont quasi-parfaits, comme 6=1+2+3, ou 28=1+2+4+7+14. Le nombre presque-parfait 12=6+4+2=6+3+2+1 n'est pas quasi-parfait ; 60 s'écrit de 34 manières différentes comme somme de certains de ses diviseurs !

Pour tout premier p impair, le nombre $2^{E(ln_2(p))}p$ est quasi-parfait : 2×3, 4×5, 4×7, 8×11, ... Mais il y en a d'autres ; les plus petits n'étant pas de cette forme sont $490 = 2 \times 5 \times 7^2$, $572 = 2^2 \times 11 \times 13$, 748, 3770, ...

Le plus petit quasi-parfait impair est $8925 = 3 \times 5^2 \times 7 \times 17$ dont la décomposition de 1 en FE associée est :

$1 =$ 1/3+1/5+1/7+1/15+1/17+1/21+1/25+1/35+1/51+1/75+1/85+1/105+1/119 +1/175+1/255+1/357+1/425+1/525+1/595+1/1275+1/2975 qui comporte 21 termes.

Je n'ai pas trouvé cette suite des quasi-parfaits dans la bibliothèque « Sloane ».

Une nouvelle formule de génération d'une infinité de décompositions de 1 en FE ; la voici : soit n un entier ; pour tout $k > 0$, pour tout d diviseur de n on a :

$$\frac{1}{n} = \sum_{i=1}^{k} \frac{1}{d(n/d+1)^i} + \frac{1}{n(n/d+1)^k}$$

exemple : pour n=6, d=2,k=3, $1/6 = 1/8 + 1/32 + 1/128 + 1/384$.

3.3 Fractions égyptiennes et nombres de Carmichael

Là c'est fin Août et début Septembre que cela se passe ; je fais de l'expérimentation puis de la bibliographie et je tombe sur l'article d'un chercheur parisien, Bernard Montaron, intitulé *Carmichael polynomials, pseudo-perfect numbers and egyptian fractions* de décembre 2003, qui fait le point sur les recherches récentes dans ce domaine.

Deux remarques à ce propos :

1- j'avais, dans une expérimentation avec « maple » fin Août, utilisé des polynômes qui se sont avérés être des cas particuliers de ces polynômes de Carmichael, piliers théoriques de cet article.

2- quelle ne fut pas ma surprise que cet auteur signale que les avancées les plus significatives dans ce domaine de recherche étaient l'œuvre de Harvey Dubner ; c'est un des quatre collègues avec qui on a réussi, en 1998, a trouvé une progression arithmétique de 10 nombres premiers consécutifs, record qui est aujourd'hui impossible à battre, au vu de la lenteur des ordinateurs.

C'est ce problème qui est source de celui que je travaille périodiquement : le nombre 19 m'intrigue.

Je vais vous résumer les idées essentielles de cet article (qui fait le point sur des recherches actuelles en lien avec les décompositions de 1 en FE).

Tout démarre avec le (petit) théorème de Fermat, théorème qui est un premier test (grossier) de primalité d'un entier :

tout nombre premier p est tel que pour tout entier n, p divise $n^p - n$.

Mais il existe des nombres qui ne sont pas premiers et vérifiant cette propriété, d'où :
Définition : Un nombre de Carmichael est un entier non premier vérifiant cette propriété. Le plus petit est $561 = 3 \times 11 \times 17$, et ces nombres de Carmichael sont caractérisés par les propriétés suivantes :
1- Tout nombre de Carmichael est le produit de k nombres premiers distincts, avec $k >= 3$.
2- Un nombre n est de Carmichael si et seulement si pour tout les diviseurs premiers p de n, p-1 divise n-1 (et la propriété 1- ci-dessus).
On sait (depuis moins de 20 ans) qu'il existe une infinité de nombres de Carmichael, mais on ne sait toujours pas s'il existe une infinité de tels nombres ayant k diviseurs premiers (k fixé, $k > 2$). Pourtant on sait que si $n = (6x+1)(12x+1)(18x+1)$, avec les trois facteurs (6x+1), (12x+1) et (18x+1) premiers, alors n est de Carmichael. Ce polynôme $P_6 = (6x+1)(12x+1)(18x+1)$ est un polynôme dit de Carmichael. Ces polynômes de Carmichael ont une définition précise (similaire à la définition d'un nombre de Carmichael) que je ne vais pas donner. Il existe un polynôme de Carmichael de degré 3, 6 de degré 4, 72 de degré 5, et vous imaginez la suite.
Le plus intéressant est de savoir que toute décomposition de 1 en FE distinctes nous donne un polynôme de Carmichael et réciproquement, le lien entre les deux passant par les nombres presque-parfaits. Ceci fut établit, en 1995, par mon collègue Harvey Dubner.
Comment passe-t-on d'une décomposition de 1 en FE à un polynôme de Carmichael ?
C'est très simple...

Retour aux Situations Connexes
Suite

Soit $1 = \frac{1}{n_1} + \frac{1}{n_2} + \ldots + \frac{1}{n_k}$ une décomposition de 1 avec $n_1 < n_2 < \ldots < n_k$; prenons $N = ppcm(n_1, n_2, \ldots, n_k)$ (qui est presque-parfait) et notons $m_i = N/n_i$; alors le polynôme de Carmichael associé est

$$P = \Pi_{i=1}^{k}(m_i\, N\, x\ +\ 1).$$

Exemple pour k=3, on a $1 = 1/2 + 1/3 + 1/6$, d'où N=6, puis $P = (6x + 1)(12x + 1)(18x + 1)$. Voici un programme (rapide) pour trouver des nombres de Carmichael à partir de la suite des facteurs d'un polynôme de Carmichael.

```
> Carmi :=proc(A)
local t,k ;
k :=nops(A) :t :=convert(map(isprime,A),set) :
if t={true} then [A,convert(A,'*')] fi ;
end :
```
A partir de P pour la décomposition $1 = 1/2 + 1/3 + 1/6$, on pose

```
>A :=[6*x+1, 12*x+1, 18*x+1] ;
```
puis on applique la procédure (ici pour les 200 premiers x).

```
>L :=[seq(Carmi(A),x=1..200)] ;
```
Voici la réponse (instantanée) donnant 10 nombres de Carmichael

$L := [[[7, 13, 19], 1729], [[37, 73, 109], 294409], [[211, 421, 631], 56052361],$
$[[271, 541, 811], 118901521], [[307, 613, 919], 172947529], [[331, 661, 991], 216821881],$
$[[337, 673, 1009], 228842209], [[601, 1201, 1801], 1299963601],$
$[[727, 1453, 2179], 2301745249], [[1171, 2341, 3511], 9624742921]].$

On peut alors tester ce que donne ces nombres modulo 30($= 2 \times 3 \times 5$) :
$>$ map(u$-$ $>$op(2,u) mod 30,L) ;

$$[19, 19, 1, 1, 19, 1, 19, 1, 19, 1]$$

on ne trouve que les nombres 1 et 19 qui est racine de 1 modulo 30, vérification en une dizaine de secondes pour plus de 1000 nombres de Carmichael obtenus avec ce polynôme. Pourquoi ?
On peut poursuivre avec les 6 polynômes associés aux 6 décompositions de 1 en quatre fractions égyptiennes ; on trouve rapidement beaucoup de nombres de Carmichael, mais cette fois ils sont égaux à 1, 7 ou 13 modulo 30 et tous égaux à 1 modulo 6=2*3 ; notons que 7 et 13 sont des racines de 19 modulo 30. Le mystère ne s'éclaircit pas, rappelons que tout nombre premier ($>$ 3 est forcément de la forme $6 \times n \pm 1$). Pour les 72 polynômes de degré 5, les nombres de Carmichael obtenus (environ 25 à 35 par polynôme) sont tous de la forme $6 \times n + 1$ et égaux à 1, 13, 19 et pour l'un d'entre eux à 7, modulo 30. Il n'y a plus de doute, le nombre 19, son carré 1 et ses deux racines carrés 13 et 7 ont un sens dans ce cadre ; il reste à le comprendre.
En bref
Pour moi, aujourd'hui, je suis persuadé que la « connaissance » des nombres premiers est un problème aussi difficile que celui de la « connaissance » des décompositions de 1 en FE, et que résoudre ce dernier est quasiment équivalent à résoudre le premier.

Le 06 septembre 2007

Retour aux Situations Connexes