Divers

Marc SAGE

Table des matières

1	Géné de aut sont int pour M_n et S_n	2
2	Fibonacci	2
3	Sur phi	3
4	Une sous-Syracuse	3
5	intégralité d'une mocheté	4
6	Produit de Dirichlet	4
7	Lemme d'Eudoxe-Archimède	5
8	Pgcd des binomiaux	5
9	Sur les entiers somme de deux carrés	6
10	Définition de la fonction d'Ackerman	6
11	GTF	6
12	Poly et Mobius	7

1 Géné de aut sont int pour M_n et S_n

Z centre de A

Heureusement, notre Directeur de Departement prefere' m'a en une seconde indique le bouquin qui fallait : "Corps non commutatifs" de Blanchard (PUF).

Et effectivement, ca marche avec le resultat suivant, qui est une extension agreable des 2 classiques analogues concernant les automorphismes de L(E) (en dimension finie) et S_n (pour n ≠ 6) :

A un corps de dimension finie sur Z, A_i deux sous-corps contenant Z, et f un isomorphisme (de Z-algebre) entre les A_i. Alors f est prolongeable en un automorphisme interieur de A.

Appliquons ici a A_1 = Z[x] qui st un Z-ev de base (1, x, x^2, ..., x^{d-1}) et A_2 pareil en y (d designant toujours le degre du polynome mini. commun), et f : x ↦ y.

A_1 est bien une algebre car x^d est Z-lie aux 1, ..., x^{d-1}, lesquele forment unebase car generatrice par definition et libre par minimalite du polynome annulateur.

f est bijective par definition, homorphisme de Z-ev trivialement et homorphisme de Z-algebre (c.a.d. pro- piete multiplicative en plus) par egalite des polynomes minimaux

Gilles Feyrit
19 déc 1991 14h39

2 Fibonacci

Write φ=(1+sqrt(5))/2. Assume that the interval [nφ - 1/n , nφ + 1/n] contains an integer. φrove that n is a Fibonacci number. (Any integer in the interval is then also Fibonacci, but that's easy.)

This problem seems straightforward. The main (hardly clever) ideas are

(i) to obtain a precise formula for the distance between F_n*φ and the nearest integer, where F_n is a Fibonacci number (just write out the closed formula for F_n); and

(ii) write an arbitrary number m as a sum of distinct Fibonacci numbers, m=F_i1+...+F_in, and check that F_i1*φ is "too far away" from any integer for the other F_i2*φ,...,F_in*φ to bring it as close as 1/m again. A technical detail is that, when one writes m like this, there are no consecutive Fibonacci terms in the sum.

Although it is indeed easy, it shall prove useful in the sequel.

Let φ = (1+√5)/2, ψ = (1-√5)/2. It is well known that the n-th Fibonacci number is

$$F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}} \text{ (avec } F_1 = F_2 = 1).$$

Also note that φ ≈ 1,618 and ψ ≈ -0,618, racine de X^2 - X - 1, d'où φ + ψ = 1, φψ = -1. This means that

$$F_n \varphi = \frac{\varphi^{n+1} + \psi^{n-1}}{\sqrt{5}} = \frac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}} + \frac{\psi^{n+1} + \psi^{n-1}}{\sqrt{5}} = F_{n+1} + \psi^{n-1} \frac{1 + \psi^2}{\sqrt{5}} \stackrel{?}{=} F_{n+1} + \psi^{n+1} (\varphi - 1).$$

En effet, ψ^2 = 1 + ψ, donc

$$\begin{aligned} \frac{1 + \psi^2}{\sqrt{5}} &= \frac{2 + \psi}{\sqrt{5}} = \frac{5 - \sqrt{5}}{2\sqrt{5}} = \frac{\sqrt{5} - 1}{2} \\ \stackrel{?}{=} \psi^2 (1 + \varphi) &= (1 + \psi)(\varphi - 1) = \varphi - 1 + (-1) - \psi = -2 + \sqrt{5} \end{aligned}$$

????

$$= F_{n+1} + \psi^{n+1} (\varphi - 1).$$

Since |ψ| < 1, F_n * φ is alternately "just below" and "just above" an integer, namely F_{n+1}. And since the norm

$$|\varphi^{n+1} (\varphi - 1) - F_{n+1}| = |\varphi - 1| |(-1)^{n+1} - \psi^{2n+2}| / \sqrt{5} = |(-1)^{n+1} - \psi^{2n+2}| * |\varphi - 1| / \sqrt{5} < 0.3,$$

the distance from $F_{-n} * \varphi$ to F_{-n+1} is less than $0.3/F_{-n+1} < 1/F_{-n}$, establishing the easy part of the claim.

Now let m be any positive integer, and write m as the sum of distinct Fibonacci numbers,

$$m = F_{i_1} + \dots + F_{i_N} \text{ (increasing, non-consecutive terms).}$$

I'm going to show that the distance from $m\varphi$ to any integer is at least $\frac{1}{F_{i_N}}$; this proves that the distance from $m\varphi$ to the nearest integer is greater than $1/m$, and thus there can be no integers in the interval $[m\varphi - 1/m, m\varphi + 1/m]$.

The proof is elementary. Earlier we saw that

$$\varphi F_n = F_{n+1} + \psi^{n+1}(\varphi - 1).$$

assume, for definiteness, that i_1 is odd, so that $F_{-i_1} * \varphi$ lies just above F_{-i_1+1} ; the other case is similar. Let us work modulo Z . We are going to see that neither the contribution of the odd indices among $i_2, \dots, i_N$ (meaning $F_{-i_2} * \varphi + \dots + F_{-i_N} * \varphi \pmod{Z}$, where the sum ranges over the odd indices), nor that of the even indices, are enough, separately, to make $m * \varphi$ very close to an integer. Since each class contributes in a different direction, taking all of them together does not change the conclusion.

The contribution mod Z of the odd indices among $i_2, \dots, i_N$ is bounded above as follows. The next sum should be understood to range over the odd elements of $\{i_2, \dots, i_N\}$:

$$(\varphi - 1)(\psi^{i_2+1} + \dots + \psi^{i_N+1}) \leq (\varphi - 1)(\psi^{i_1+3} + \psi^{i_1+5} + \dots) \leq (\varphi - 1)(-\psi)^{i_1+2}$$

Adding that to the initial contribution of $F_{-i_1} * \varphi$, we get

$$(\varphi - 1)\psi^{i_1+1} + (\varphi - 1)(-\psi)^{i_1+2} = (\varphi - 1)(1 - \psi)\psi^{i_1+1} = \psi^{i_1+1}$$

$$(\varphi - 1) * \psi^{\wedge\{i_1+1\}} + (\varphi - 1) * -\psi^{\wedge\{i_1+2\}} = (\varphi - 1) * (1 - \psi) * \psi^{\wedge\{i_1+1\}} = \psi^{\wedge\{i_1+1\}}.$$

Since $\psi^2 < 1/2$, $\psi^{\wedge\{i_1+1\}}$ is closer to 0 than to 1 (mod Z); and the distance, $\psi^{\wedge\{i_1+1\}}$, is manifestly greater than $1/F_{-i_1+2}$ (the first odd index greater than i_1).

On the other hand, the even indices among $i_2, \dots, i_N$ can't bring $F_{-i_1} * \varphi$ close to 0 either. The next sum ranges over the even indices in $\{i_2, \dots, i_N\}$:

$$\begin{aligned} & (\varphi - 1) * (\psi^{\wedge\{i_2+1\}} + \dots + \psi^{\wedge\{i_N+1\}}) < \\ & < (\varphi - 1) * (\psi^{\wedge\{i_1+4\}} + \psi^{\wedge\{i_1+6\}} + \psi^{\wedge\{i_1+8\}} + \dots) = \\ & = (\varphi - 1) * -\psi^{\wedge\{i_1+3\}}. \end{aligned}$$

(We start the second sum at $\psi^{\wedge\{i_1+4\}}$ because $\psi^{\wedge\{i_1+2\}}$ would mean consecutive Fibonacci terms.)

Now,

$$\begin{aligned} & (\varphi - 1) * \psi^{\wedge\{i_1+1\}} + (\varphi - 1) * -\psi^{\wedge\{i_1+3\}} = (\varphi - 1) * \psi^{\wedge\{i_1+1\}} * (1 - \psi^2) = \\ & = (\varphi - 1) * -\psi^{\wedge\{i_1+2\}} = (1 + \psi) * \psi^{\wedge\{i_1+1\}}, \end{aligned}$$

and this is greater than $1/F_{-i_1+3}$ (the first even index greater than i_1).

3 Sur phi

Tiens, je fais un léger non-sequitur pour mentionner la question suivante (qui, à ce que je sache, est encore ouverte) : est-il vrai que pour tout naturel n non nul il existe $a \neq n$ tel que $\varphi(a) = \varphi(n)$?

C'est facile de prouver que c'est vrai pour tout n jusqu'à une valeur assez grande (genre, deux millions) : je donnais ça en khôlle à une certaine époque.

David, 25 janvier 2005 22h05

4 Une sous-Syracuse

Soit $f : N \rightarrow N$ définie par $f(n) = \frac{n}{2}$ si n est pair, $f(n) = \frac{3n+1}{2}$ si n est impair. Je pars de $n_0 > 0$ et je construis $n_i := f^{o_i}(n_0)$ par itération de f .

Montrer que si je me fixe une suite finie de longueur N d'éléments de $\{\text{pair, impair}\}$, il existe un n_0 tel que les N premières valeurs de n_i ont les parités correspondantes. (Autrement dit, je peux trouver n_0 pour imposer la parité de n_0 , de n_1 , de n_2 , etc., tant que j'en mets un nombre fini.)

Pour tout entier naturel i , la valeur de $f(n)$ modulo 2^i ne dépend que de n modulo 2^{i+1} ; par conséquent, la parité de n_k ne dépend que de n_0 modulo 2^{k+1} . Par récurrence sur N , admettons que l'on ait trouvé un n_1 tel que la parité de la suite des $n_1, n_2 = f(n_1), \dots, n_N$ soit donnée par les parités imposées $p_1, \dots, p_N$. Dans le cas favorable, on voudrait trouver un n_0 antécédent de n_1 par f qui ait la parité p_0 . Si p_0 est pair, en prenant $p_0 = 2p_1$, c'est fait. Sinon, d'après la remarque ci-dessus, on se rend compte que l'on a le droit de remplacer n_1 par un élément qui lui est congru modulo une puissance de 2 suffisamment grande, ce qui permet de supposer que la division nécessaire à l'obtention de n_0 tombe juste.

5 intégralité d'une mocheté

Recherche la solution la plus élégante du problème suivant (je ne sais pas en fait, si on peut définir l'élégance d'une solution, et si tel est le cas, si une telle solution existe, mais bon).

Montrer que $(1 + \sqrt{2})^n + (1 - \sqrt{2})^n$ est entier.

Posons $x_n = (1 + \sqrt{2})^n + (1 - \sqrt{2})^n$

1) On développe avec le binôme de Newton

2) On remarque que la suite définie par :

$$u_0 = 2, \quad u_1 = 2$$

$$u_{n+2} = 2u_{n+1} + 1$$

coïncide avec x_n et est « entière »

3) On considère la matrice $M = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$ qui a pour valeurs propres $1 + \sqrt{2}$ et $1 - \sqrt{2}$. Donc $x_n = \text{tr } M^n$ est entier.

4) On considère la conjugaison dans $\mathbb{Z}[\sqrt{2}]$ qui est un morphisme, d'où le résultat

5) On pose $P(X) = (1+X)^n + (1-X)^n$. P est pair donc peut s'écrire $Q(X^2)$ où est un polynôme à coefficients entiers. Ainsi $P(\sqrt{2}) = Q(2)$ est entier.

6) $1 + \sqrt{2}$ et $1 - \sqrt{2}$ sont les deux racines du polynôme $(X - 1)^2 - 2$ qui est à coefficients entiers. Ton expression étant symétrique en ces deux nombres elle s'exprime à l'aide des fonctions symétriques élémentaires qui sont des entiers. Les coefficients sont entiers parce que c'est une somme de Newton.

7) $1 + \sqrt{2}$ et $1 - \sqrt{2}$ sont des entiers algébriques donc l'expression est un entier algébrique; comme c'est aussi un rationnel (conjugaison), c'est un entier rationnel.

Bon d'accord il y en a quatre sur les six qui ont déjà été proposées... Ce que j'aurais aimé comprendre, c'est pourquoi un tel problème admet ces nombreuses solutions a priori si diverses et s'il y en a une parmi celles-ci (ou pas d'ailleurs) qui est plus fondamentale que les autres, c'est-à-dire qui nous montre bien pourquoi ça marche...

6 Produit de Dirichlet

Tu as une bijection canonique entre N et les suites d'entiers à support fini par la décomposition en facteurs premiers. On peut donc associer à une fonction f une série formelle $\sum_n f(n) \prod X_i^{a_i}$ où $n = \prod p_i^{a_i}$ et réciproquement.

La loi de multiplication se transporte par cette opération sur la loi de multiplication usuelle des séries formelles $\mathbb{C}[[X_1, X_2, \dots]]$ qui si je ne m'abuse, est un anneau local, puisque ses éléments non inversibles forment un idéal maximal.

Les fonctions multiplicatives sont en bijection avec leurs valeurs sur les $p_i^{a_i}$: les éléments correspondants dans $\mathbb{C}[[X_1, \dots]]$ sont exactement les éléments qui s'écrivent comme produit infini de f_i avec f_i dans $\mathbb{C}[[X_i]]_1$ (éléments de terme constant 1)

Ainsi le groupe *Mult* des fonctions multiplicatives est canoniquement isomorphe au produit infini des groupes $\mathbb{C}[[X_i]]_1$.

Or celui-ci, par l'application logarithme (algèbres de Lie, mumble...), est isomorphe au groupe additif des séries formelles nulles en zéro, c'est-à-dire l'idéal maximal $z\mathbb{C}[[z]]$, qui est canoniquement isomorphe en tant que groupe additif à $\mathbb{C}[[z]]$ lui-même.

Ainsi *Mult* est isomorphe à $(\mathbb{C}[[z]], +)^{\aleph_0}$. On remarque ainsi qu'il est muni d'une structure naturelle de $\mathbb{C}[[z]]$ -module, et que c'est un "groupe de Lie" de dimension infinie, qui correspond sur le groupe multiplicatif puissance $\aleph_0$ à "mettre à la puissance f ". Je ne veux pas essayer de trouver l'opération correspondante sur les fonction multiplicatives.

Et donc tout bidule non trivial engendre un groupe isomorphe à $\mathbb{Z}$.

On peut interpréter chacune des fonctions multiplicatives citées comme des séries formelles. Certaines ont la propriété d'être invariantes par une permutation des nombres premiers, donc ce sont des produits infinis de séries formelles identiques en $X_1, X_2, \dots$

$$1 \rightarrow \text{produit des } 1 + z + z^2 + \dots = \frac{1}{1-z}$$

$$\delta \rightarrow \text{produit des } 1$$

$$\mu \rightarrow \text{produit des } (1 - z)$$

$$\tau \rightarrow \text{produit des } 1 + 2z + 3z^2 \dots = \frac{1}{(1-z)^2}$$

Ceux-là sont sur la même droite.

D'autres dépendent des nombres premiers :

$$\text{Id} \rightarrow \text{produit des } 1 + pz + p^2 z^2 \dots = \frac{1}{1-pz}$$

$$\varphi \rightarrow \text{produit des } 1 + \sum (p_i^{\alpha_i} (1 - \frac{1}{p_i}) X_i^{\alpha_i}) = 1 + \frac{(1 - \frac{1}{p_i}) X_i}{1 - p_i X_i}$$

$$\sigma \rightarrow \text{produit des } 1 + (1+p)z + (1+p+p^2)z^2 \dots = (1+z+\dots) + p(z+\dots) + p^2(z^2+\dots) = \frac{1}{(1-z)(1-pz)}$$

$$\sigma_k \text{ (somme des diviseurs à la puissance } k) \rightarrow \frac{1}{(1-z)(1-p^k z)}$$

On constate ainsi que ceux-là sont linéairement indépendants, sauf σ qui est $\frac{\text{Id}}{\mu} = \text{Id} * 1$

Mais après, certains cas ne ressemblent vraiment plus à rien et cela me semble infaisable de continuer à la main.

J'ignore si la question a déjà été traitée et si elle est d'un intérêt quelconque...

Je ne crois pas que ça ait grand intérêt, à part peut-être trouver des identités remarquables. Mais bon, la technique de séries génératrices que j'ai expliquée juste au-dessus trivialisait tellement la chose que ça doit être complètement éculé. Si quelqu'un connaît des résultats étonnants ou références, ça peut être amusant.

7 Lemme d'Eudoxe-Archimède

c'est bien d'Eudoxe de Cnide que je parle, et une bonne raison pour laquelle le lemme ne peut pas être dû à Archimède est qu'il figure dans les **Éléments** d'Euclide (définitions V.4 et V.5 et proposition X.1), donc soit Archimède était sacrément précoce soit Euclide avait le don de prescience. En fait, on considère généralement que c'est à Eudoxe que sont dus les résultats du livre X des **Éléments** (si ce n'est les énoncés eux-mêmes).

Ce qui ne veut pas dire qu'Archimède n'a pas contribué des choses dans l'histoire (peut-être pour le généraliser, comme pour l'appliquer à des courbes ou à des aires), et on appelle parfois ce truc « lemme d'Eudoxe-Archimède » (<URL : <http://eom.springer.de/A/a013090.htm> > mentionne les deux noms). Il semble que l'idée de mettre le nom d'Archimède dans l'affaire est apparue au XIXe (O. Stolz, « Zur Geometrie der Alten, insbesondere über ein Axiom des Archimedes », **Math. Annalen** 22 (1883), 504-519 : je ne suis pas allé vérifier cette référence ;-). Mais Archimède lui-même, dans l'introduction de **La Quadrature de la parabole** attribue le lemme à des géomètres plus anciens (<URL : <http://www.math.ubc.ca/~cass/archimedes/parabola/para234.html> >, premières lignes de la page), pensant sans doute à Eudoxe (il le cite nommément dans l'introduction de **La Sphère et le Cylindre**, mais à propos d'autre chose).

Ce qui me surprend un peu, c'est que ça surprenne : je croyais que c'était complètement standard, au moins en anglais, de parler de lemme d'Eudoxe, mais je n'y vois aucune référence par exemple sur Wikipédia.

8 Pgcd des binomiaux

Est-il vrai que le pgcd des coefficients binomiaux $\binom{n}{i}$ pour n fixé et i allant de 1 à $n-1$ est :
 p si $n = p^m$, p premier

1 sinon ?

Ça paraît relativement raisonnable. C'est un diviseur de n par hypothèse. Soit p un diviseur premier de n , et i tel que $p^i | n$ mais pas p^{i+1} .

Si $p^i < n$, alors le coef. bin. $\binom{n}{p^i}$ n'est pas multiple de p (on compte soigneusement les puissances de p et ça passe (ou legendre...))

Et donc le pgcd vaut 1.

Si $n = p^i$, le raisonnement ci-dessus permet de prouver que le pgcd vaut au plus p (en considérant $\binom{n}{p^{i-1}}$).

Pareil, on compte encore soigneusement et ça doit passer.

On considère un nombre n s'écrivant sous la forme qp^m avec p premier ne divisant pas q . Comme $\binom{n}{1} = n$, le pgcd divise n . On va montrer que p ne divise pas le pgcd cherché, et après on applique ça sur tous les p qui divisent n .

Pour ça on calcule la valuation p -adique de $\binom{n}{p^m}$ qui vaut

$$\begin{aligned} & \sum_{k \neq 1} \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k \neq 1} \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k \neq 1} \left\lfloor \frac{n - p^m}{p^k} \right\rfloor \\ &= \sum_{k=0}^{m-1} p^k (q-1) + \sum_{k \neq 1} \left\lfloor \frac{q}{p^k} \right\rfloor - \sum_{k=0}^{m-1} (q-1)p^k - \sum_{k \neq 1} \left\lfloor \frac{q-1}{p^k} \right\rfloor \\ &= \sum_{k \neq 1} \left(\left\lfloor \frac{q}{p^k} \right\rfloor - \left\lfloor \frac{q-1}{p^k} \right\rfloor \right) \end{aligned}$$

Mais comme p ne divise pas q , chacun des derniers termes de cette somme vaut 0, donc la valuation cherchée vaut 0, et p ne divise pas $\binom{n}{p^m}$.

9 Sur les entiers somme de deux carrés

Tous ses facteurs premiers congrus à 3 modulo 4 apparaissent avec un exposant pair. Les nombres premiers congrus à 3 modulo 4 sont précisément ceux qui ne se scindent pas dans $\mathbb{Z}[i]$.

10 Définition de la fonction d'Ackerman

$$\begin{aligned} f(0,m) &= m+1 \\ f(n,0) &= n+1 \\ f(n+1,m+1) &= f(n, f(n+1,m)) \end{aligned}$$

11 GTF

Les nombres premiers p qui satisfont $p^2 \mid 2^p - 1$ s'appellent les nombres premiers de Wiefrich, et jusqu'à présent les deux seuls qu'on connaisse sont 1093 et 3511. Leurs écritures en base deux sont assez marrantes.

L'intérêt de ces nombres vient du théorème suivant :

Théorème (Wiefrich, 1909) :

Soit p un nombre premier qui n'est PAS de Wiefrich. Alors le premier cas de FLT est vrai pour p .

12 Poly et Mobius

Soit $P \in Z[X]$ et $n > 0$. Soit $Q := \sum_{dd'=n} \mu(d) P(X^d)^{d'}$. Alors tous les coefficients de Q sont multiples de n .

E.g. Si $P = b + cX$ et $n = 6$, on a

$$\begin{aligned} Q &= P(X)^6 - P(X^2)^3 - P(X^3)^2 + P(X^6) \\ &= X^6(c^6 - c^3 - c^2 + c) + X^5(6bc^5) \\ &\quad + X^4(15b^2c^4 - 3bc^2) + X^3(20b^3c^3 - 2bc) \\ &\quad + X^2(15b^4c^2 - 3b^2c) + X(6b^5) + b^6 - b^3 - b^2 + b \end{aligned}$$

and the coefficients of Q are all multiples of 6, for whatever b and c .

Two hints at how to prove it :

Being free to add a multiple of n to each coefficient of f , we may assume that all those coefficients are positive.

POur tous entiers s et $n > 0$, la somme entière $\sum_{dd'=n} \mu(d) s^{d'}$ est le nombre d'applications $f : Z/nZ \rightarrow Z/sZ$ telles que pour tout $x \in Z/nZ$ il y a un $y \in Z/nZ$ tq $f(x+y) \neq f(y)$ (meaning, the function k is not fixed by any nonzero translation of its domain). That number is a multiple of n because the f 's fall into equivalence classes each of which has n elements.