LES $\mathcal{M}$ATHS : L'Ω ?

Organe officiel de la Régionale de CAEN de l'APMEP : **Numéro 11 - Janvier 2011**
Rédacteur en Chef : Richard Choulet

Éditorial. Cette fois, qu'on se le dise : 2011 est premier ! Par ailleurs l'itérée « somme des carrés des chiffres » donne : 6, 36, 45, 41, 17, 50, 25, 29, 85, $\cdots$ et après ? Que donne pour 2011, l'algorithme RATS de l'Ω 7 ? C'est vous qui voyez et encore bonne année pleine de rebondissements mathématiques pour ne pas trop perdre de votre capital cérébral. Commençez par vérifier que

$$229033559540535250662023353193782376059688 90+5107320211161387136750185662322016053209 97\sqrt{2011}$$

est une unité dans $\mathbb{Q}(\sqrt{2011}$ (voyez ce bon `http://www.alpertron.com/CUAD.HTM`).

****

LES NOUVELLES Les journées de l'APMEP

Bien studieux les anciens !

Perplexe

Grande sauterie à la mairie

Congressistes enjouées

Voire hilare

Soyons sérieux un peu !

****

N'oubliez pas que : une association est d'autant plus forte qu'elle a de nombreux adhérents. Les seules ressources de l'APMEP sont les cotisations de ses membres et la vente des brochures qu'elle diffuse. Les enseignants de mathématiques qui souhaitent lire les bulletins de l'APMEP sont d'autant plus vivement invités à adhérer qu'ils bénéficient sur le montant de l'adhésion (hors abonnement) d'une réduction fiscale de 66% au titre de don aux oeuvres d'intérêt général. Les formules (adhésion + abonnements) et tout particulièrement la formule « Tout APMEP » sont toutes plus avantageuses que les abonnements hors adhésion. Par exemple l'adhésion Tout APMEP pour un titulaire du second degré revient à 45 euro.

****

Lecture d'autrefois

Possédant encore quelques vieux numéros du « Petit Archimède » des années octante, je propose, au fil des Ω de vous livrer quelques articles curieux, insolites $\cdots$. « LE PETIT ARCHIMÈDE » était la revue de « l'Association pour le Développement de la Culture Scientifique » dont le Président était Yves Roussel. La mention du texte que je propose est : « D'après une idée de J.-C. H » dans le numéro 95-96 du PA d'octobre 1983 (Jean Claude Herz était alors le directeur de la publication).

LES VERTUS DU NOMBRE 7

Il n'y a pas si longtemps encore le PA (n°88-89 page 28) rappelait les propriétés remarquables de 142857, suite des chiffres qui se présentent dans la division de 1 par 7. *(NdlR On y faisait calculer n fois ce nombre magique ($1 \leqslant n \leqslant 6$) pour observer l'apparition des chiffres composant 142857 tandis qu'avec $n = 7$, on avait $\cdots$.)*

Nous nous intéressons ici aux chiffres successifs du quotient par 7 du nombre 142857 142857 $\cdots$, soient 2, 0, 4, 0, 8, 1, 6, 3, 2, 6, 5, $\cdots$.

Ainsi :

$$0,142857142857\cdots = 7 \times 0,02040816326\cdots .$$

Le résultat est étonnant avec toutes ces puissances de deux. Il l'est moins si on considère :

$$\frac{2}{100} + \left(\frac{2}{100}\right)^2 + \left(\frac{2}{100}\right)^3 + \cdots = \frac{2}{100} \times \frac{1}{1 - \frac{2}{100}} = \frac{1}{49} = \frac{\frac{1}{7}}{7}.$$

On aurait plus de décimales encore si on écrivait :

```
02.4.8163264|
          1|   28|
               2|   56|
                    5|   12
                             .    ...
020408163265     30    61    .    ....
```

****

Solution de l'exercice de l'Ω 10

Je rappelle l'énoncé : *ABC est un triangle équilatéral d'aire T. D un point de la droite (BC) tel que B soit sur [DC]. C_1 est le cercle inscrit dans DAB et C_2 le cercle exinscrit à DAC et tangent à [AC]. La somme des aires des disques limités par C_1 et C_2 est notée S.*

1. Montrer que la somme des diamètres de C_1 et C_2 est indépendante de la position de D.

2. Déterminer l'ensemble des valeurs prises par S/T.

3. Construire à la règle et au compas un point D de (BC) tel que $S/T = \dfrac{5\pi\sqrt{3}}{9}$.

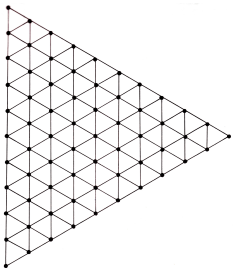
Claude Dujardin s'est concentré sur l'exercice dès qu'il a reçu l'Ω et m'a envoyé sa solution qui est analytique. Il prend ABC direct et le repère d'origine A pour lequel les coordonnées des points sont B($\frac{a}{2}$; $\frac{a\sqrt{3}}{2}$) et C($-\frac{a}{2}$; $\frac{a\sqrt{3}}{2}$). D, quant à lui, aussi sur la droite d'équation $y = tx$ avec $t = \tan\frac{\theta}{2} \in]0\ ;\ \frac{\sqrt{3}}{3}[$ a pour coordonnées ($\frac{a\sqrt{3}(1-t^2)}{4t}$; $\frac{a\sqrt{3}}{2}$).

Après quelques calculs, il trouve la somme des rayons des deux cercles : $r_1 + r_2 = \frac{a\sqrt{3}}{2}$, indépendante de t. Puis vient ensuite le calcul de S=$\frac{3\pi a^2(1+3t^2)}{8}$ puis $\frac{\mathrm{S}}{\mathrm{T}} = \frac{\sqrt{3}\pi(1+3t^2)}{2} \in]\frac{3\pi a^2}{8};\ 2\pi a^2[$. La condition imposée à la dernière question donne alors $t = \frac{\sqrt{3}}{9}$. Notre collègue termine avec $\frac{\theta}{2} \approx 11°20'$. Un programme GeoGebra pour faire la figure serait le bienvenu !

****

L'exercice du numéro 11

Cet exercice a aussi été proposé au PETIT ARCHIMÈDE (octobre 82) mais je l'avais déjà dans mes cartons à l'époque. Le voici, le voilà : c'est du brutal. Combien y a-t-il de triangles, de parallélogrammes dans la figure ci-dessous ? Généralisez.



****

La demi-journée de la régionale

Elle aura lieu le **mercredi 6 avril après-midi** au collège Lemière à Caen avec pour conférencier Yves Ducel-Fages, maître de conférences à l'IREM de Franche-Comté qui viendra parler de « Mise en perspective des programmes de troisième et seconde en probabilités ». Il se propose à partir de l'analyse des derniers programmes, d'étudier, en l'illustrant dans des activités pédagogiques, la continuité de l'enseignement des probabilités des classes de troisième et de seconde.

Un programme détaillé de cette après-midi là vous sera communiqué ultérieurement.

****

Notre page publicitaire

Demander, recommander, emprunter sans le rendre le tome 1 de « Mieux consommer grâce aux mathématiques » de l'IREM de Caen avec pour auteurs Gilles Damamme, Évelyne Adam et Hélène Ventelon édité par les célèbres éditions Hermann au prix de 19,50 euro. Qu'on se dise ! Le tome 2, destiné au lycée cette fois, est en préparation.

Coup de cœur aussi pour le jeu MATHISTO (12 euro), jeu de cartes édité par CIJM (Comité International des Jeux Mathématiques), déjà loué dans le dernier BGV : pour commander s'adresser à la trésorière de la régionale.

****

Des idéaux principaux aux algorithmes *par Jacques Faisant*

L'ensemble $\mathbb{Z}$[i] des nombres complexes de la forme $a + \mathrm{i}.b$ où a et b appartiennent à $\mathbb{Z}$ est appelé l'ensemble des entiers de Gauss ; c'est un anneau intègre dans lequel il est assez amusant d'essayer de « faire de l'arithmétique » ; pour débuter, voici quelques remarques.

Premières remarques concernant les entiers de Gauss

Les éléments inversibles de $\mathbb{Z}[i]$ sont 1, -1, i et $-\mathrm{i}$; en effet, leurs inverses respectifs sont 1, -1, $-\mathrm{i}$ et i.

Et il n'en existe pas d'autre ; on peut le voir en employant la norme ; la norme d'un entier de Gauss z est $N(z) = z.\bar{z}$; ce n'est pas la norme de la géométrie mais on a quand même $N(z_1.z_2) = N(z_1).N(z_2)$; ainsi, si $(a + \mathrm{i}.b).(a' + \mathrm{i}.b') = 1$, alors $N(a + \mathrm{i}.b).N(a' + \mathrm{i}.b') = (a^2 + b^2).(a'^2 + b'^2) = N(1) = 1$. Donc la norme d'un entier de Gauss inversible est nécessairement un naturel qui divise 1 ; on dit que les entiers de Gauss z et z' sont associés, lorsque $z' = uz$, où u est un entier de Gauss inversible.

On a $2 = (1 + \mathrm{i}).(1 - i)$; donc on dit que $1 + \mathrm{i}$ est un diviseur de 2 et que, donc, 2 n'est pas premier ... dans $\mathbb{Z}$[i] ! Pour éviter une confusion, on peut utiliser le mot irréductible plutôt que le mot premier pour les entiers de Gauss : un entier de Gauss z est irréductible si et seulement si toute égalité $z = z_1.z_2$ où z_1 et z_2 sont des entiers de Gauss implique que z_1 ou z_2 est un entier de Gauss inversible.

Quels sont les entiers de Gauss irréductibles ?

Définissons deux conditions concernant un entier de Gauss z :

C_1 : la norme de z est un entier naturel premier

C_2 : z est associé à un entier naturel premier congru à 3 modulo 4

On peut montrer que : z est irréductible si et seulement si il vérifie C_1 ou C_2.

Contentons-nous pour l'instant de cette affirmation non démontrée ; ceci sera le thème d'un article à venir, relié à la question de l'écriture d'un naturel entier premier sous la forme de la somme des carrés de deux entiers.

Dans $\mathbb{Z}[i]$, on peut définir une adaptation de la division euclidienne de $\mathbb{Z}$: étant donnés des entiers de Gauss x et y avec $y \neq 0$, il existe des entiers de Gauss q et r tels que $x = y.q + r$ et $N(r) < N(y)$. On peut le voir en écrivant $\frac{x}{y} = t + \mathrm{i}.u$ où t et u appartiennent à $\mathbb{Q}$ et en notant a l'entier « le » plus proche de t, b l'entier « le » plus proche de u et $q = a + \mathrm{i}.b$; on a alors $x = y.q + r$ avec $r = y.(t + \mathrm{i}.u) - y.(a + \mathrm{i}.b) = y.(t - a + \mathrm{i}.(u - b))$ et $N(r) = N(y).((t - a)^2 + (u - b)^2) < N(y)$ car $(t - a)^2 + (u - b)^2 \leqslant \frac{1}{2}$ et $N(y) > 0$.

Exemple : pour $x = 3, y = 2, q = 2$ et $r = -1$ si on dit que 2 est l'entier « le » plus proche de 1,5 puisque $3 = 2.2 - 1, N(-1) = 1 < 4 = N(2)$ ou bien : $q = 1$ et $r = 1$ si on dit que 1 est l'entier « le » plus proche de 1,5 puisque $3 = 2.1 + 1, N(1) = 1 < 4 = N(2)$. Il n'y a pas unicité !

Mais l'existence de cette division euclidienne dans $\mathbb{Z}$[i] permet de démontrer que tous les idéaux de $\mathbb{Z}$[i] sont de la forme $g.\mathbb{Z}$[i] (idéal engendré par g) où g est un élément de $\mathbb{Z}$[i] ; (l'anneau des entiers de Gauss est donc un anneau principal). Ceci permet de définir le pgcd de deux entiers de Gauss z_1 et z_2 : c'est un générateur g de l'idéal $z_1.\mathbb{Z}[\mathrm{i}] + z_2.\mathbb{Z}[\mathrm{i}]$ de $\mathbb{Z}$[i] engendré par z_1 et z_2. Ce pgcd n'est donc pas défini de manière unique mais, comme deux de ces pgcd g_1 et g_2 se divisent l'un l'autre, on a $g_1 = z_1.g_2$ et $g_2 = z_2.g_1$ où, donc, z_1 et z_2 sont inversibles. On peut donc décider arbitrairement qu'on prendra comme pgcd celui des quatre entiers de Gauss possibles dont la partie réelle et la partie imaginaire sont des naturels positifs ou nuls (pgcd dans le premier quadrant du plan complexe). La division euclidienne dans $\mathbb{Z}$[i] évoquée plus haut permet de calculer « le » pgcd de deux entiers de Gauss, en suivant les étapes de l'algorithme d'Euclide dans $\mathbb{Z}$.

Algorithmes

Avec l'arrivée probable d'une spécialité informatique, il semble bon de se pencher sur l'algorithmique. Les remarques ci-dessus rendent possible certains calculs ; profitons-en pour développer puis implémenter des algorithmes.

Représentation des entiers de Gauss

Dans un premier temps, nous nous servirons de logiciels de calcul formel ; dans ce cas, nous utiliserons le type de données « nombre complexe » que possèdent ces logiciels. Il faudra être certain que les parties entières et imaginaires utilisées sont des entiers relatifs.

Calcul de la norme d'un entier de Gauss

Un algorithme peut être généralement décomposé en trois parties : acquisition des données, traitement, sortie des résultats. Cette description grossière suffit ici.

Autrefois, on décrivait les algorithmes à l'aide d'un organigramme mais cela conduisait, dit-on, au style de programmation « go to » qui est abandonné.

On décrit maintenant un algorithme à l'aide d'un pseudo-langage de programmation, facile à comprendre, le seul symbole pas forcément connu étant « := » qui représente l'affectation d'une valeur à une variable.

Algorithme du calcul de la norme de $z \in \mathbb{Z}$[i] :

$u := z$
$n := u.\bar{u}$
sortie de n

C'est simple ; passons à plus compliqué !

Algorithme du calcul de celui des éléments associés à l'entier de Gauss z qui est dans le premier quadrant du plan complexe

On a dit que deux entiers de Gauss étaient associés si et seulement si l'un est égal au produit de l'autre par un élément inversible (1, -1, i ou −i). Il a été affirmé précédemment que tout entier de Gauss, z, a un élément associé situé dans le premier quadrant ; démontrons-le et l'algorithme recherché en découlera. (Voici un argument en faveur de la connaissance des démonstrations !)

Il y a un cas très simple : il se peut que z soit dans le premier quadrant ; dans ce cas, comme z est associé à lui-même, la réponse est obtenue sans calcul ; le cas où z est dans le troisième quadrant n'est guère moins simple : on utilise une symétrie centrale ; cette symétrie centrale est aussi une rotation et on voit bien deux autres rotations qui conviennent pour les deux cas restants. Il s'agit donc de savoir dans quel quadrant est z et de faire l'opération complexe correspondant à la transformation *ad hoc*. Dans l'algorithme ci-dessous, nous utiliserons des instructions de contrôle « si ... alors ... sinon ... » imbriquées.

$u := z$
si $Re(u) > 0$ alors
    si $Im(u) > 0$ alors
        $c := u$
    sinon
        $c :=$ i.u
sinon
    si $Im(z) > 0$ alors
        $c := -$i.u
    sinon
        $c := -u$
sortie de c

L'imbrication des instructions « si ... alors ... sinon ... » n'est clairement définie que grâce à l'indentation de certaines lignes par rapport aux autres ; le langage de programmation Python (langage à la mode !) est basé sur l'indentation, mais c'est le seul. Pour tout autre langage, une syntaxe spécifique doit être employée.

Algorithme du calcul « du » quotient et « du » reste de la division euclidienne d'un entier de Gauss x par un autre, y

De la définition vue précédemment découle l'algorithme figurant en annexe 1 ; vous pouvez l'écrire vous même.

Algorithme du calcul du pgcd normalisé de deux entiers de Gauss x et y

On écrit l'algorithme d'Euclide dans $\mathbb{Z}$[i] ; le fait que ce soient, ici, non pas les restes de division mais les normes des restes de division qui sont de plus en plus petits, garantit quand même la validité de l'algorithme ; le dernier reste sera nul puisque sa norme sera nulle.

$a := x$
$b := y$
si $N(a) < N(b)$ alors
    échange de a et b
si $b = 0$ alors
    si $a = 0$ alors
        fin avec message d'erreur
    sinon
        fin et sortie de la valeur normalisée de a
sinon
    tant que $b \neq 0$ faire
        $c =$ reste de la division euclidienne de a par b
        $a := b$
        $b := c$
fin et sortie de la valeur normalisée de a

Algorithme indiquant si un entier de Gauss z est irréductible ou non

Rappelons que z est irréductible si et seulement si il vérifie C_1 ou C_2 avec :

C_1 : la norme de z est un entier naturel premier
C_2 : z est associé à un entier naturel premier congru à 3 modulo 4

De cela découle l'algorithme figurant en annexe 2 ; vous pouvez l'écrire vous même.

Algorithme déterminant tous les entiers de Gauss qui sont irréductibles et dont la norme est inférieure ou égale à un naturel *borne* donné

Nous pouvons utiliser une liste pour représenter le résultat à obtenir, étant donné que les logiciels de calcul formel possèdent ce type de données. On utilise deux variables ayant des valeurs entières, s et t, et une variable ayant une liste d'entiers de Gauss comme valeur, l.

$a :=$ *borne*
$l :=$ liste vide
pour s variant, par pas de 1, de 0 jusqu'à la partie entière de la racine carrée de *borne* faire
    $t := 0$
    tant que la norme de l'entier de Gauss $s + \mathrm{i}.t$ est inférieure ou égale à *borne* faire
        si $s + \mathrm{i}.t$ est irréductible alors
            ajouter à la fin de la liste l
        augmenter de 1 la valeur de t
sortie de l.

Il est très important de remarquer que l'avant-dernière ligne de l'algorithme est indentée de deux espaces, alors que la dernière ligne ne l'est pas du tout.

On peut réécrire cet algorithme en utilisant davantage de symboles :

$a :=$ *borne*
$l := []$
pour $s := 0$ jusqu'à partie entière (racine carrée(*borne*)) faire
    $t := 0$
    tant que norme$(s + \mathrm{i}.t) \leqslant$ *borne* faire
        si $s + \mathrm{i}.t$ est irréductible alors
            $l :=$ *append*$(l, s + \mathrm{i}.t)$
        $t := t + 1$
sortie de l

Appelons *irréductibles* cet algorithme.

Algorithme donnant un diviseur du complexe *z*

$t := z$
$l :=$ liste des entiers de Gauss irréductibles dont la norme est inférieure ou égale à norme(t)
$i := 1$
tant que le reste de la division euclidienne de t par l[i] est non nul faire
    $i := i + 1$
sortie de l[i]

Appelons *diviseur* cet algorithme.

Algorithme déterminant la factorisation d'un entier de Gauss *z* en éléments irréductibles

$t := z$
$N :=$ norme(t)
$l :=$ *irréductibles*(N)
$L := []$
tant que norme(t) est différent de 1 faire
    $s :=$ *diviseur*(t)
    $l :=$ *append*(L, s)
    $t := \frac{t}{s}$
mettre la dernière valeur de t en tête de L
sortie de L

Explication : la division $\frac{t}{s}$ dans $\mathbb{C}$ donne un entier de Gauss, puisque s est un diviseur de t ; lorsque la norme de t vaut 1, tous les irréductibles de la décompostion de z ont été obtenus, chacun autant de fois que nécessaire, mais le produit de tous ces irréductibles n'est à priori pas égal à z ; par contre, en multipliant encore par la dernière valeur de t, (valeur qui est un inversible), on obtient z et il est donc intéressant de mettre cet inversible dans le résultat.

Conclusions

1. Il reste à écrire ces algorithmes dans un ou des langages de programmation (Maple, Maxima, Javascript ...) ; en attendant la suite de cet article, on peut aller visiter le site http ://pagesperso-orange.fr/jacques.faisant/Entiers_de_Gauss/

2. Ce qui peut être intéressant et qui ne se voit pas automatiquement, c'est le rôle des mathématiques dans l'efficacité d'un algorithme ; en effet, on pourrait écrire :

Algorithme *peu efficace* **indiquant si un entier de Gauss z est irréductible ou non**

$a := z$
$irred := vrai$
$borne :=$ norme(a)
pour $s := 0$ jusqu'à la partie entière de la racine carrée($borne$) faire
    $t := 0$
    tant que $irred$ est vrai et que norme($s + \mathrm{i}.t$) $< borne$ faire
        si norme($s + \mathrm{i}.t$) > 1 et le reste de la division euclidienne de a par $s + \mathrm{i}.t$ est nul alors
            $irred := faux$
        augmenter t de 1
sortie de $irred$

Cet algorithme va être très lent si la norme de z est grande (3,42 secondes pour tester l'irréductibilité de $299 + 24\mathrm{i}$) , contrairement à celui qui est basé sur les conditions C_1 ou C_2 (moins de un centième de seconde).

3. Question qu'on peut alors se poser : sur quel résultat mathématique un algorithme efficace de décomposition d'un entier premier congru à 3 modulo 4 comme somme de deux carrés pourrait-il reposer ?

À suivre ...

Annexe

Annexe 1 : algorithme du calcul « du » quotient et « du » reste de la division euclidienne d'un entier de Gauss x par un autre, y

$a := x$
$b := y$
si $b = 0$ alors
    fin avec message d'erreur
$q := \frac{a}{b}$
$q := arrondi(Re(q)) + \mathrm{i}.arrondi(Im(q))$
$r := a - b.q$
sortie de la liste composée de q puis r

(La fonction « arrondi » est censée donner l'entier le plus proche d'un rationnel donné, ou d'un réel flottant donné).

Annexe 2 : Algorithme indiquant si un entier de Gauss z est irréductible ou non

$a :=$ entier de Gauss associé à z mais qui est dans le premier quadrant
si la norme de a est un entier premier alors
    sortie de $vrai$
sinon
    si a est un réel, donc un entier, est premier et est congru à 3 modulo 4 alors
        sortie de $vrai$
    sinon
        sortie de $faux$

Bibliographie

D. Guin et T. Hausberger : Algèbre I, groupes, corps et théorie de Galois, EDP Sciences, 2008.

****

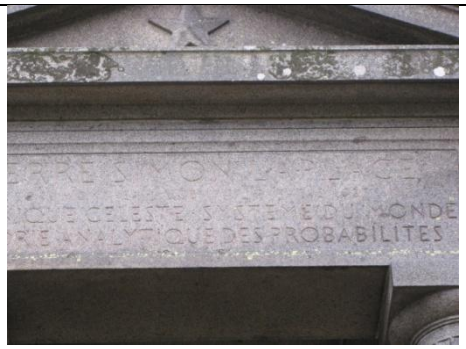
Les adresses utiles

La Présidente : annie.memin@ac-caen.fr La Trésorière : ch.faisant@wanadoo.fr
Les Secrétaires : nadine.lucas@laposte.net, delevalle@wanadoo.fr Le scribe : richard.choulet@orange.fr
Le site national avec notre petit coin local : `www.apmep.asso.fr` ; `www.apmep.asso.fr/spip.php?rubrique58`
et aujourd'hui

****

Notre page culturelle

	Le saviez-vous ? Nous les aborigènes mathématiciens, savons tous, plus ou moins, que Pierre Simon de Laplace est né en 1749 à Beaumont en Auge. Il est peut-être un peu moins connu qu'il est mort en 1827 à Paris. Et maintenant la question à mille euro : maizou gît donc sa tombe ? Réponse qui ne pourra que vous élever en société : au fin fond d'un champ, à Saint Julien de Mailloc, petit village du pays d'Auge situé entre Lisieux et Orbec, dont notre intrépide reporter (le taureau normand est un sournois quand on le réveille) a rapporté quelques images.

 Le mausolée	 Le fronton	 L'urne funéraire
 Le trou étoilé de la porte	 Le buste de Laplace par Guillaume	 Son château