Calcule et ... (Denise Vella-Chemla, juillet 2022)

On reprend notre exemple fétiche de la recherche des décomposants de Goldbach de l'entier pair $n = 98$.

$$S_{98} = \begin{cases} 98 \equiv 0 \pmod 2 \\ 98 \equiv 2 \pmod 3 \\ 98 \equiv 3 \pmod 5 \\ 98 \equiv 0 \pmod 7 \end{cases}$$

Appelons d_{98} un décomposant de Goldbach potentiel de $n = 98$. d_{98} peut être congru, hormis 0, à tout ce à quoi $n = 98$ n'est pas congru. Le signe $\vee$ dans le système ci-dessous est à lire comme un ou exclusif, son emploi étendu est à comprendre comme le fait de vérifier autant de systèmes de congruences que la combinatoire le permet.

$$S_{d_{98}} = \begin{cases} d_{98} \equiv 1 \pmod 2 \\ d_{98} \equiv 1 \pmod 3 \\ d_{98} \equiv 1 \vee 2 \vee 4 \pmod 5 \\ d_{98} \equiv 1 \vee 2 \vee 3 \vee 4 \vee 5 \vee 6 \pmod 7 \end{cases}$$

Remarque : on notera que le fait de respecter le système de systèmes de congruences ci-dessus est une condition suffisante mais non nécessaire pour être un décomposant de Goldbach de n. On trouvera la preuve de cette caractérisation des décomposants de Goldbach d'un nombre pair n qui sont supérieurs à la racine carrée de n en [1].

Comme on peut le comprendre, les modules qui ne divisent pas n "éliminent davantage de classes de congruences" (au nombre de 2) que les modules qui divisent n. Plaçons-nous dans le pire des cas, où l'on élimine deux classes de congruences par module premier inférieur à $\sqrt{n}$, on trouve tout de même

$$\frac{1}{2} \prod_{\substack{p \text{ premier} \\ 5 \leq p \leq \sqrt{n}}} (p-2)$$

classes de congruences différentes par l'application du théorème des restes chinois à chacun des systèmes de congruences combinatoirement trouvé (voir $S_{d_{98}}$ ci-dessus). La division par 2 est justifiée par les symétries autour des moitiés (par exemple, pour 40, les classes de congruences trouvées par l'application du théorème des restes chinois à chaque système[1] sont les classes $30k+11, 30k+17, 30k+23$ et $30k+29$ dont on ne conserve que la moitié par symétrie autour de 20, la moitié de 40.

Mais d'autre part, les solutions étant toutes des unités du groupe $(\mathbb{Z}/n\mathbb{Z})^{\times}$, la moitié d'entre elles sont inférieures à $D = \dfrac{1}{2} \displaystyle\prod_{\substack{p \text{ premier} \\ 3 \leq p \leq \sqrt{n}}} p$ (pour illustrer cela sur l'exemple $n = 98$, la moitié des solutions (s'il en existe) sont forcément inférieures à $105 = 3 \times 5 \times 7$).

[1]Systèmes de congruences pour $n = 40$:

$$\begin{cases} 40 \equiv 0 \pmod 2 \\ 40 \equiv 1 \pmod 3 \\ 40 \equiv 0 \pmod 5 \end{cases} \qquad S_{d_{40}} = \begin{cases} d_{40} \equiv 1 \pmod 2 \\ d_{40} \equiv 2 \pmod 3 \\ d_{40} \equiv 1 \vee 2 \vee 3 \vee 4 \pmod 5 \end{cases}$$

Serait-il possible de "rater l'intervalle visé", i.e. que toutes les solutions soient supérieures à n, comprises entre n et D ?

Imaginons qu'il existe un corps K dont on serait assuré qu'une de ses extensions E/K contienne l'une des solutions (on n'a pas trouvé d'équation polynomiale générale que seuls les décompoosants de Goldbach de n satisferaient). L'existence d'un décomposant de Goldbach pourrait découler d'une minoration trouvée dans [2] p. 7. Le théorème de densité assure l'existence d'un certain nombre de nombres premiers inférieurs à une certaine borne, et ce qui garantirait l'existence d'un décomposant de Goldbach serait que cette borne soit inférieure à n.

Le manque de technique en mathématiques est très handicapant.

Référence

[1] D. Chemla, *Réécrire*, http://denise.vella.chemla.free.fr/jade1.pdf

[2] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publications Mathématiques de l'IHÉS, Tome 54 (1981), pp. 123-201.

Annexe : extraits de [2] fournissant la minoration (p. 5 et 7)

§ 1. Majorations de discriminants

1.1. Notations

Soit K un corps de nombres algébriques, autrement dit une extension finie de $\mathbf{Q}$. On pose :

A_K anneau des entiers de K,
$n_K = [K : \mathbf{Q}] = [A_K : \mathbf{Z}] =$ degré de K,
$\sum_K$=ensemble des places ultramétriques de K,
$d_K =$ valeur absolue du discriminant de K.

Si $v \in \sum_K$, on identifie v à la valuation discrète normée correspondante (de groupe des valeurs $\mathbf{Z}$), et l'on note $\mathfrak{p}_v$, l'idéal premier de A_K qui correspond à v. Le corps résiduel $A_K/\mathfrak{p}_v$, est un corps fini; on note p_v sa caractéristique, et Nv le nombre de ses éléments. On a

$$Nv = N\mathfrak{p}_v = (p_v)^{f_v},$$

où f_v est le degré résiduel de v. L'indice de ramification e_v de v est défini par $e_v = v(p_v)$; c'est le plus grand entier positif e tel que $\mathfrak{p}_v^e$ divise p_v.

Soit E une extension finie de K, de degré $n = n_E/n_K = [E : K]$. On note $\mathfrak{D}_{E/K}$ (resp. $\mathfrak{d}_{E/k}$) la différente (resp. le discriminant) de l'extension E/K ; c'est un idéal $\neq 0$ de A_E (resp. A_K). On a
(1) $$\mathfrak{d}_{E/K} = N_{E/K}(\mathfrak{D}_{E/K}) \qquad \text{et} \qquad d_E = (d_K)^n N(\mathfrak{d}_{E/K}),$$

cf. par exemple [38], chap. III.

1.2. Estimations locales

Soit E/K comme ci-dessus, et soit $w \in \sum_E$ une place ultramétrique de E. Notons v la place de K induite par w, et soit $e_{w/v} = e_w/e_v$ l'indice de ramification de w par rapport à v. On s'intéresse à *l'exposant* $w(\mathfrak{D}_{E/K})$ de l'idéal premier $\mathfrak{p}_w$ dans la différente $\mathfrak{D}_{E/K}$:

Proposition 1. On a

$$w(\mathfrak{D}_{E/K}) = e_{w/v} - 1 + s_{w/v}, \qquad \textit{avec} \qquad 0 \leq s_{w/v} \leq w(e_{w/v}).$$

[...]

En appliquant la prop. 1, on en déduit

$$\begin{aligned} v(\mathfrak{d}_{E/K}) &= \sum_{w|v} f_{w/v}(e_{w/v} - 1) + \sum_{w|v} f_{w/v} s_{w/v} \\ &\leq \sum_{w|v} f_{w/v} e_{w/v} - 1 + \sum_{w|v} f_{w/v} e_w v_p(e_{w/v}) \\ &\leq n - 1 + n e_v \operatorname*{Sup}_{w|v} v_p(e_{w/v}), \end{aligned} \tag{2}$$

du fait que $n = \sum_{w|v} f_{w/v} e_{w/v}$.

[...]

D'autre part, comme E/K est ramifiée en v, on a $e \geq 2$, et la formule (2) ci-dessus montre que

$$v(\mathfrak{d}_{E/K}) \geq gf(e-1) \geq n(1 - 1/e) \geq n/2.$$