Retour aux polynômes de Tchebychev ainsi que d'autre part aux indices de la section 53 des Recherches arithmétiques de Gauss (Denise Vella-Chemla, 9.5.2019)

1) Cosinus, divisibilité, symbole de Kronecker

On voudrait revenir ici sur la possibilité de calculer les cosinus d'un multiple entier d'un angle en utilisant le polynôme de Tchebychev $T_2(x)$ de première espèce et de degré 2, ce qui permet, en utilisant un symbole de Kronecker, de calculer les booléens de divisibilité qu'on a utilisés à plusieurs reprises.

On rappelle que les polynômes de Tchebychev sont définis par la récurrence suivante :

$$\begin{cases} T_0(x) = 1 \\ T_1(x) = x \\ T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \end{cases}$$

En particulier, le polynôme de Tchebychev de degré 2 est égal à $T_2(x) = 2x^2 - 1$.

On a utilisé pour modéliser la divisibilité de x par y le nombre $\cos\left(\frac{2\pi x}{y}\right)$ qu'on réécrit, pour le considérer comme un multiple entier d'angle comme $\cos\left(2\left(\frac{\pi x}{y}\right)\right)$ et l'on peut obtenir la valeur de ce cosinus par le polynôme $T_2(x)$ en la variable $\cos\left(\frac{\pi x}{y}\right)$.

Si on se place dans le plan complexe, on utilisera plutôt la représentation du cosinus comme moyenne de deux complexes :

$$\cos\left(\frac{\pi x}{y}\right) = \frac{e^{\frac{i\pi x}{y}} + e^{-\frac{i\pi x}{y}}}{2}$$

Ci-dessous, on fournit un programme de calcul en python des cosinus par cette méthode.

```
#include <iostream>
#include <stdio.h>
#include <math.h>
#include <complex.h>

typedef std::complex<double> dcomp;
const double PI = acos(-1.0);

double T_rec(int n, double x) {
  if (n == 0) return 1.0;
  if (n == 1) return x;
  return 2.0 * x * T_rec(n-1, x) - T_rec(n-2, x);
}

int main (int argc, char* argv[])
{
  double err = 1.e-8;
  int n = 10;

  for (int y = 1; y <= n; ++y) {
    for (int x = 1; x <= n; ++x) {
      double z = cos(PI*(double)x/(double)y);
      double t = T_rec(2, z);
      std::cout << x << ", " << y << " --> " << t << "\n" ;
    }
    std::cout << "\n" ;
  }
}
```

Le résultat de ce programme pour x et y variant de 1 à 10 est fourni plus loin.

Le cosinus pour x et y vaut bien sûr 1 lorsque x divise y et un nombre différent de 1 dans les autres cas. Pour obtenir à la place du cosinus un booléen de divisibilité d'un nombre x par un nombre y, on pourra utiliser le symbole de Kronecker $\delta_1^i(T_2(cos(\pi x/y)))$ qui vaut 1 si $T_2(cos(\pi x/y)) = 1$ et 0 sinon.

La définition de cette fonction de divisibilité permet de caractériser les nombres premiers (leur somme de cosinus sur tous les nombres qui leur sont strictement inférieurs vaut 1).

Cette fonction prend les valeurs suivantes :

x | y	1	2	3	4	5	6	7	8	9	10
1	1	0	0	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0	0	0
3	1	0	1	0	0	0	0	0	0	0
4	1	1	0	1	0	0	0	0	0	0
5	1	0	0	0	1	0	0	0	0	0
6	1	1	1	0	0	1	0	0	0	0
7	1	0	0	0	0	0	1	0	0	0
8	1	1	0	1	0	0	0	1	0	0
9	1	0	1	0	0	0	0	0	1	0
10	1	1	0	0	1	0	0	0	0	1

Cosinus calculés par le programme utilisant le polynôme de Tchebychev

Voici le résultat du programme pour x et y variant de 1 à 4.

```
1 , 1 --> 1
2 , 1 --> 1
3 , 1 --> 1
4 , 1 --> 1
5 , 1 --> 1
6 , 1 --> 1
7 , 1 --> 1
8 , 1 --> 1
9 , 1 --> 1
10 , 1 --> 1

1 , 2 --> -1
2 , 2 --> 1
3 , 2 --> -1
4 , 2 --> 1
5 , 2 --> -1
6 , 2 --> 1
7 , 2 --> -1
8 , 2 --> 1
9 , 2 --> -1
10 , 2 --> 1

1 , 3 --> -0.5
2 , 3 --> -0.5
3 , 3 --> 1
4 , 3 --> -0.5
5 , 3 --> -0.5
6 , 3 --> 1
7 , 3 --> -0.5
8 , 3 --> -0.5
9 , 3 --> 1
10 , 3 --> -0.5

1 , 4 --> -1.03412e-13
2 , 4 --> -1
3 , 4 --> 3.10679e-13
4 , 4 --> 1
5 , 4 --> -5.16614e-13
6 , 4 --> -1
7 , 4 --> 7.24325e-13
8 , 4 --> 1
9 , 4 --> -9.3026e-13
10 , 4 --> -1
```

2) Indices de Gauss, cardinaux d'ensembles de nombres qui sont racines d'équations identiques

On cherche une caractérisation claire des nombres premiers de la forme $4k+3$: on a du mal à en trouver une dans la littérature alors que tous connaissent le fait qu'un nombre premier de la forme $4k+1$ se décompose de manière unique en une somme de deux carrés [1].
On calcule les indices associés à chaque nombre modulo un certain entier n. Les indices en question sont expliqués dans l'article 53 des recherches arithmétiques.

53. Pour nous faire entendre plus facilement, nous présenterons d'abord un exemple. Soit $p=19$, les nombres $1, 2, 3 \ldots 18$ peuvent se distribuer de la manière suivante relativement aux diviseurs de 18 :

$$1\{1,\quad 2\{18,\quad 3\left\{\begin{matrix}7\\11\end{matrix}\right.,\quad 6\left\{\begin{matrix}8\\12\end{matrix}\right.,\quad 9\left\{\begin{matrix}4,\ 5,\ 6\\9,\ 16,\ 17\end{matrix}\right.,\quad 18\left\{\begin{matrix}2,\ 3,\ 10\\13,\ 14,\ 15\end{matrix}\right.$$

Ainsi dans ce cas $\downarrow 1=1$, $\downarrow 2=1$, $\downarrow 3=2$, $\downarrow 6=2$, $\downarrow 9=6$, $\downarrow 18=6$. Avec une légère attention on voit qu'il y en a, relativement à chaque exposant, autant qu'il y a de nombres premiers avec cet exposant et non plus grands que lui, ou bien, en reprenant le signe du n° 40, que $\downarrow d=\phi d$. Mais on peut démontrer généralement cette observation de la manière suivante :

L'analyse des données fait comprendre cet article ainsi : l'ensemble des nombres premiers à n est constitué d'un certain nombre de parties disjointes. Chaque partie contient des nombres dont la même puissance est congrue à l'unité modulo n (on mettra par exemple dans un même ensemble les nombres dont la puissance 7ème vaut 1). La somme des cardinaux des différentes parties est égale à $\varphi(n)$ l'indicateur d'Euler de n.
L'analyse de ce résultat fournit la caractérisation suivante pour les nombres premiers :

- *un nombre premier p de la forme $4k+3$ est tel que les ensembles de nombres qui sont premiers à p et dont une même puissance vaut 1 sont appariables par leur cardinalité ;*

- *il en est de même pour une puissance d'un nombre premier p de la forme $4k+3$ (on peut apparier les ensembles de nombres de même puissance égale à l'unité dans le corps premier $\mathbb{Z}/p\mathbb{Z}$ par bijection (i.e. ils sont 2 par 2 de même cardinal) ;*

- *un nombre premier p de la forme $4k+1$ est tel que l'un de ses ensembles de nombres qui sont premiers à p et dont une même puissance vaut 1 n'est appariable à aucun autre par sa cardinalité.*

Cardinalité des ensembles de mêmes puissances égales à l'unité, pour les nombres impairs entre 10 et 20

Le premier exemple est à lire ainsi : 2^{10} et 6^{10} sont égaux à 1 modulo 10, ou encore 3^5. Ces nombres dont une même puissance vaut 1 sont à imaginer comme étant placés dans un même ensemble et les

1. Théorème démontré par Fermat, Euler, Gauss (cf. http://denisevellachemla.eu/Gauss-4k+1-RA182.pdf et Don Zagier "A one-sentence proof that every prime $p \equiv 1$ (*mod* 4) is a sum of two squares", *Amer. Math. Monthly*, 97 (2) :144, 1990.)

cardinaux de ces ensembles valent ici 4, 4, 1 et 1 (indiqués après la flèche à droite de 10).

```
11  →  4,  4,  1,  1
10  :  2  6  7  8
 5  :  3  4  5  9
 2  :  10
 1  :  1

13  →  4,  2,  2,  2,  1,  1
12  :  2  6  7  11
 6  :  4  10
 4  :  5  8
 3  :  3  9
 2  :  12
 1  :  1

15  →  4,  3,  1
 4  :  2  7  8  13
 2  :  4  11  14
 1  :  1

17  →  8,  4,  2,  1,  1
16  :  3  5  6  7  10  11  12  14
 8  :  2  8  9  15
 4  :  4  13
 2  :  16
 1  :  1

19  →  6,  6,  2,  2,  1,  1
18  :  2,  3,  10,  13,  14,  15
 9  :  4,  5,  6,  9,  16,  17
 6  :  8,  12
 3  :  7,  11
 2  :  18
 1  :  1
```

Si maintenant on se contente de reporter les cardinaux des ensembles (à droite des flèches ci-dessus) pour les impairs de 3 à 99, on voit apparaître cette propriété d'appariement des ensembles de même cardinaux pour les premiers de la forme $4k+3$ ainsi que pour leurs puissances. Ces appariements sont symbolisés par des points-virgules et les nombres de forme $4k+3$ ou leurs puissances colorés en bleu.

3 : 1/1	23 : 10/10, 1/1	43 : 12/12, 6/6, 2/2, 1/1	63 : 24, 8, 3, 1	83 : 40/40, 1/1
5 : 2, 1, 1	25 : 8, 4, 4, 2, 1, 1	45 : 8, 6, 4, 3, 2, 1	65 : 24, 12, 6, 3, 2, 1	85 : 32, 16, 12, 3, 1
7 : 2/2, 1/1	27 : 6/6, 2/2, 1/1	47 : 22/22, 1/1	67 : 20/20, 10/10, 2/2, 1/1	87 : 24, 18, 6, 4, 3, 1
9 : 2/2, 1/1	29 : 12, 6, 6, 2, 1, 1	49 : 12, 12, 6, 6, 2, 2, 1, 1	69 : 30, 10, 3, 1	89 : 40, 20, 10, 10, 4, 2, 1, 1
11 : 4/4, 1/1	31 : 8/8, 4/4, 2/2, 1/1	51 : 16, 8, 4, 3, 1	71 : 24/24, 6/6, 4/4, 1/1	91 : 32, 24, 8, 4, 3, 1
13 : 4, 2, 2, 2, 1, 1	33 : 12, 4, 3, 1	53 : 24, 12, 12, 2, 1, 1	73 : 24, 12, 8, 6, 6, 4, 4, 2, 2, 2, 1, 1	93 : 24, 12, 8, 6, 4, 3, 2, 1
15 : 4, 3, 1	35 : 8, 6, 4, 3, 2, 1	55 : 16, 12, 4, 4, 3, 1	75 : 16, 12, 4, 4, 3, 1	95 : 24, 18, 8, 6, 6, 4, 3, 2, 1
17 : 8, 4, 2, 1, 1	37 : 12, 6, 6, 4, 2, 2, 2, 1, 1	57 : 18, 6, 6, 3, 2, 1	77 : 24, 12, 8, 6, 4, 3, 2, 1	97 : 32, 16, 16, 8, 8, 4, 4, 2, 2, 2, 1, 1
19 : 6/6, 2/2, 1/1	39 : 8, 6, 4, 3, 2, 1	59 : 28/28, 1/1	79 : 24/24, 12/12, 2/2, 1/1	99 : 24, 12, 8, 6, 4, 3, 2, 1
21 : 6, 3, 2, 1	41 : 16, 8, 4, 4, 4, 2, 1, 1	61 : 16, 8, 8, 8, 4, 4, 4, 2, 2, 2, 1, 1	81 : 18/18, 6/6, 2/2, 1/1	