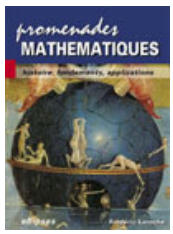

accueil

La fonction Phi d'Euler

L'arithmétique qui fut un des sujets les plus attractifs pour les Grecs fut oubliée pendant près de quatorze siècles : de Diophante (vers 200 ap. J.- C.) à Pierre de Fermat (vers 1650) il n'y eut pratiquement aucun résultat nouveau de découvert. Ce dernier s'intéressa plutôt à la résolution d'équations diophantiennes (les équations à résoudre en nombres entiers) et laissa de côté une partie fondamentale de l'étude des nombres entiers : la question de leurs diviseurs.

Cent ans plus tard Euler reprit une partie du travail de Fermat et commença à développer cette branche : on lui doit de nombreux résultats et théorèmes en Théorie des Nombres.

Prenons un nombre entier comme 200 : si on effectue sa décomposition en facteurs premiers on obtient $200 = 2^3 5^2$; tous ses diviseurs seront alors constitués de toutes les puissances de 2 et 5, lesdites puissances étant comprises entre 0 et 3 pour 2, 0 et 2 pour 5.

En fait il est facile de voir que les diviseurs sont alors

$$2^0 5^0,\ 2^1 5^0,\ 2^2 5^0,\ 2^3 5^0,\ 2^0 5^1,\ 2^1 5^1,\ 2^2 5^1,\ 2^3 5^1,\ 2^0 5^2,\ 2^1 5^2,\ 2^2 5^2,\ 2^3 5^2\ ;$$

ils sont donc au nombre de $4.3 = 12$.

Généralisons : un nombre N s'écrit $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ où les p_i sont des nombres premiers ; le nombre de ses diviseurs est alors

$$\phi(N) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_n + 1)\,.$$

Faisons maintenant le produit de deux nombres ayant chacun deux facteurs premiers dont un en commun :

$$N = a^\alpha b^\beta\ ,\ M = a^{\alpha'} c^\gamma \text{ et } NM = a^\alpha b^\beta a^{\alpha'} c^\gamma = a^{\alpha+\alpha'} b^\beta c^\gamma\ ,$$

on a alors

$$\phi(N) = (\alpha+1)(\beta+1)\ ,\ \phi(M) = (\alpha'+1)(\gamma+1) \text{ et } \phi(NM) = (\alpha+\alpha'+1)(\beta+1)(\gamma+1)\,.$$

Y-a-t'il un lien entre les deux ?

On peut évidemment écrire $\phi(NM) \le \phi(N)\phi(M)$ avec égalité lorsque N et M sont premiers entre eux puisque dans ce cas tous les facteurs premiers de l'un sont différents des facteurs premiers de l'autre.

Inversement si on prend un nombre N quel est le nombre d'entiers, noté $\varphi(N)$, qui sont premiers avec lui ? On a par exemple $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, …

Cette fonction est appelée *indicatrice d'Euler* et joue un grand rôle dans l'étude des nombres premiers.

Première constatation, si N est un nombre premier, il est divisible par 1 et par lui-même, on a donc $\varphi(N) = N - 1$; de même si on prend deux entiers premiers entre eux, on a $\varphi(NM) = \varphi(N)\varphi(M)$: d'après ce que nous avons dit précédemment $\varphi(N)$ est en fait le nombre de produits dans $\phi(N)$ et l'égalité $\phi(NM) = \phi(N)\phi(M)$ entraine $\varphi(NM) = \varphi(N)\varphi(M)$.

Supposons maintenant que N est de la forme p^k avec p premier : tous les nombres de la forme p, $2p$, $3p$,… $(p^{k-1} - 1)p$ ont un facteur commun avec N : ils sont donc au nombre de $p^{k-1} - 1$.

Vérifions avec $N = 2^3 = 8$: on a 2, 4, 6, soit 3 nombres non premiers avec N. Comme il y a $p^k - 1$ nombres inférieurs à N, il reste au total $(p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$ nombres premiers avec N et

$$\varphi(N) = p^k\left(1-\frac{1}{p}\right).$$

Nous pouvons maintenant conclure grâce à la multiplicativité de φ : si

$$N = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$$

alors

$$\varphi(N) = \varphi(p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2})\ldots\varphi(p_n^{k_n})$$

d'où

$$\varphi(N) = p_1^{k_1}\left(1-\frac{1}{p_1}\right)p_2^{k_2}\left(1-\frac{1}{p_2}\right)\ldots p_n^{k_n}\left(1-\frac{1}{p_n}\right) = N\prod_{k=1}^{n}\left(1-\frac{1}{p_k}\right).$$

Grâce à un petit programme écrit en Maple nous allons voir la fonction φ.

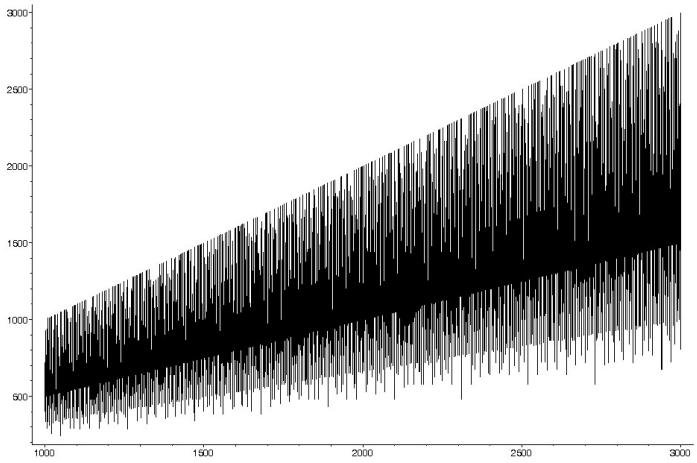

fig. 1 : Indicatrice d'Euler, $1000 \le n \le 2000$

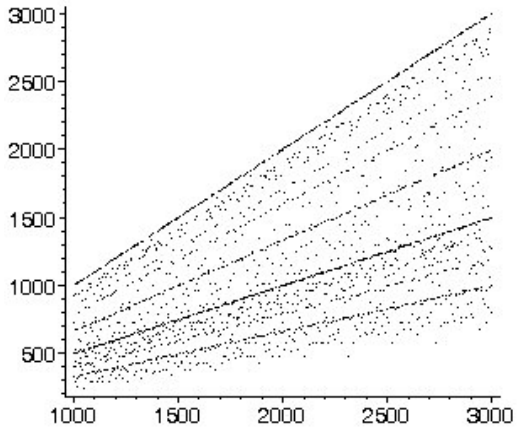

fig. 2 : Indicatrice d'Euler (points)

Voici le programme Maple :

```
> compte:= proc(n)
> local c, i, L;
> c:=0;
> for i from 1 to n-1 do
    L:=igcd(n,i);
```

```
    if (L=1) then c:=c+1; fi;
                  #ou bien end if ;
  od; #ou end do; suivant les versions
> c;
> end:
# petite procédure calculant le nombre d'entiers premiers avec n.
> n:=1000; m:=3000; L:=NULL;
> for i from n to m do L:=L,[i,compte(i)]; od:
> plot([L],color=black, font=[HELVETICA,10]);
> plot([L],color=black,style=POINT, symbol=CIRCLE, symbolsize=2,
font=[HELVETICA,10]);
```

(le # signale un commentaire non pris en compte par Maple.)

La deuxième représentation fait apparaître des droites : celle du dessus correspond aux nombres premiers qui ont le plus de non-diviseurs. On peut alors chercher quels sont les nombres correspondant aux autres alignements… et quels sont ceux qui ont le moins de non-diviseurs.

Reprenons $N = p^k$, p premier, et calculons la somme de l'indicatrice d'Euler appliquée à TOUS les diviseurs de N ; ce sont évidemment les nombres $1, p, p^2, \ldots, p^k$ et on cherche :

$$S(N) = \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^k) = 1 + p\left(1 - \frac{1}{p}\right) + p^2\left(1 - \frac{1}{p}\right) + \ldots + p^k\left(1 - \frac{1}{p}\right),$$

soit

$$S(N) = 1 + p\left(1 - \frac{1}{p}\right)(1 + p + p^2 + \ldots + p^{k-1}) = 1 + p\left(\frac{p-1}{p}\right)\frac{p^k - 1}{p-1} = 1 + p^k - 1 = N.$$

Prenons maintenant un nombre constitué d'un produit de deux termes : $N = a^n b^m$, tous les diviseurs sont de la forme $a^i b^j$ et la somme des diviseurs de N est :

$$\begin{aligned} s(a^n b^m) &= a^0 b^0 + a^1 b^0 + \ldots + a^n b^0 + a^0 b^1 + \ldots + a^n b^1 + \ldots + a^0 b^m + \ldots + a^n b^m \\ &= (a^0 + a^1 + \ldots + a^n) b^0 + \ldots + (a^0 + a^1 + \ldots + a^n) b^m \\ &= (a^0 + a^1 + \ldots + a^n)(b^0 + b^1 + \ldots + b^m) = \left(\frac{a^{n+1} - 1}{a - 1}\right)\left(\frac{b^{m+1} - 1}{b - 1}\right) = s(a^n) s(b^m). \end{aligned}$$

Appliquons exactement la même chose avec φ :

$$\begin{aligned} s[\varphi(a^n b^m)] &= \varphi(a^0 b^0) + \varphi(a^1 b^0) + \ldots + \varphi(a^n b^m) \\ &= [\varphi(a^0) + \varphi(a^1) + \ldots + \varphi(a^n)]\varphi(b^0) + \ldots + [\varphi(a^0) + \ldots + \varphi(a^n)]\varphi(b^m) \\ &= [\varphi(a^0) + \ldots + \varphi(a^n)][\varphi(b^0) + \ldots + \varphi(b^m)] = s[\varphi(a^n)] s[\varphi(b^m)]. \end{aligned}$$

Comme ceci est évidemment valable avec un nombre quelconque de termes dans N, on conclut que

$$S(N) = \sum_{d \mid n} \varphi(d) = N.$$

Il est quand même très étonnant que N puisse s'écrire comme la somme du nombre de termes premiers qui compose chacun de ses diviseurs… mais ça se sont les miracles des suites géométriques !

On termine avec un dernier résultat ; le théorème de Fermat se généralise de la manière suivante : si N est premier avec a, alors $a^{\varphi(N)} \equiv 1(N)$ (la démonstration en est laissée au lecteur).