

# Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

27/10/2011

## 1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair  $p$  est un décomposant de Goldbach de  $n$  un nombre pair supérieur ou égal à 6 si  $p$  n'est pas congru à  $n$  selon tout module premier impair  $p'$  inférieur à  $\sqrt{n}$ . En effet, dans le cas contraire, le complémentaire à  $n$  de  $p$  est composé.

*Exemple* : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car  $3 \equiv 98 \pmod{5}$  (ce qui correspond au fait que 5 divise  $98 - 3$ ). 5 n'est pas un décomposant de Goldbach de 98 car  $5 \equiv 98 \pmod{3}$ . 7 n'est pas un décomposant de Goldbach de 98 car  $7 \equiv 98 \pmod{7}$  (ce qui correspond au fait que 7 divise  $98 - 7$ , 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car  $11 \equiv 98 \pmod{3}$ . 13 n'est pas un décomposant de Goldbach de 98 car  $13 \equiv 98 \pmod{5}$ . 17 n'est pas un décomposant de Goldbach de 98 car  $17 \equiv 98 \pmod{3}$ .

## 2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach  $p$  d'un nombre pair  $n$  revient donc simplement à chercher un nombre qui vérifie les conditions suivantes : d'une part, il est premier et d'autre part, son complémentaire à  $n$  est premier.

Lors de ces recherches autour de la conjecture de Goldbach, comme il s'agit de trouver les solutions entières d'équations, on a longuement buté sur un extrait de Galois qui écrit : "*Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à  $Fx = 0$  et à  $x^{p-1} = 1$* ". Récemment, on a pu trouver sur la toile la référence [2] dans laquelle Libri explique sa méthode simple pour trouver les solutions entières d'une équation polynomiale. On réalise à ces lectures que les nombres premiers 3, 5, 7 et 11, par exemple, sont tous racines de l'équation polynomiale

$$(x - 3)(x - 5)(x - 7)(x - 11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$26 = 3 + 5 + 7 + 11.$$

$$236 = 3 \cdot 5 + 3 \cdot 7 + 3 \cdot 11 + 5 \cdot 7 + 5 \cdot 11 + 7 \cdot 11.$$

$$886 = 3 \cdot 5 \cdot 7 + 3 \cdot 5 \cdot 11 + 3 \cdot 7 \cdot 11 + 5 \cdot 7 \cdot 11.$$

$$1155 = 3 \cdot 5 \cdot 7 \cdot 11.$$

Plus généralement, pour exprimer que  $x$ , le nombre à chercher, est premier, on utilise une équation polynomiale de la forme suivante :

$$x^{\pi(n)-1} - \sigma_1 \cdot x^{\pi(n)-2} + \sigma_2 \cdot x^{\pi(n)-3} - \sigma_3 \cdot x^{\pi(n)-4} + \dots = 0$$

La plus grande puissance de  $x$  est  $\pi(n) - 1$  où  $\pi(n)$  est la notation habituelle pour le nombre de nombres premiers inférieurs à  $n$ , le  $-1$  servant à éliminer le nombre premier 2. Les nombres  $\sigma_i$  désignent respectivement les sommes de produits de  $i$  nombres premiers pris parmi tous les nombres premiers impairs considérés. Par exemple,  $\sigma_1 = p_1 + p_2 + p_3 + p_4 \dots = 3 + 5 + 7 + 11 \dots$ ,  $\sigma_2 = p_1 p_2 + p_1 p_3 + \dots + p_2 p_3 + p_2 p_4 + \dots$  et le dernier  $\sigma$  est le produit de tous les nombres premiers impairs inférieurs à  $n$ .

Pour exprimer que  $n - x$ , le complémentaire du nombre à chercher doit être l'un des nombres premiers 3, 5, 7 ou 11, on utilise la même équation polynomiale en remplaçant  $x$  par  $n - x$  ; si l'on considère les 4 premiers nombres premiers impairs seulement, l'équation polynomiale devient :

$$((n - x) - 3)((n - x) - 5)((n - x) - 7)((n - x) - 11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$(n - x)^4 - 26(n - x)^3 + 236(n - x)^2 - 886(n - x) + 1155 = 0.$$

L'élévation aux différentes puissances du monôme  $n - x$  donne les résultats ci-dessous :

$$\begin{aligned} (n - x)^4 &= x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4. \\ (n - x)^3 &= -x^3 + 3nx^2 - 3n^2x + n^3. \\ (n - x)^2 &= n^2 - 2nx + x^2. \end{aligned}$$

On reconnaît les coefficients du binôme  $C_i^j$  dans l'élévation de  $n - x$  à la puissance  $i$ .

Si on développe et qu'on regroupe ensemble les coefficients concernant une même puissance de  $x$ , on obtient :

$$x^4 + (-4n + 26)x^3 + (6n^2 - 78n + 236)x^2 + (-4n^3 + 78n^2 - 472n + 886)x + (n^4 - 26n^3 + 236n^2 - 886n + 1155) = 0$$

On reconnaît dans la dernière parenthèse le polynôme initial dans lequel  $x$  a été remplacé par  $n$ . Puis pour les coefficients des puissances supérieures de  $x$ , on voit qu'on dérive successivement le polynôme initial puis les polynômes obtenus, qu'on prend l'opposé du résultat à chaque fois et qu'on divise successivement les résultats intermédiaires par 2, 3, etc.

Pour le degré 4, le polynôme initial est :

$$n^4 - 26n^3 + 236n^2 - 886n + 1155$$

On le dérive et on en prend l'opposé :

$$-4n^3 + 78n^2 - 472n + 886$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 2 :

$$6n^2 - 78n + 236$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 3 :

$$-4n + 26$$

Les coefficients d'expression  $\frac{(-1)^n P^{(n)}(x)}{n!}$  sont appelés coefficients du développement de Taylor.

On est donc systématiquement ramené au système d'équations à deux équations de degré  $i$  suivant, dont il faudrait réussir à prouver qu'il admet systématiquement au moins une solution :

$$\begin{cases} P(x) : x^{\pi(n)-1} - \sigma_1 \cdot x^{\pi(n)-2} + \sigma_2 \cdot x^{\pi(n)-3} - \sigma_3 \cdot x^{\pi(n)-4} + \dots = 0 \\ \sum_{i=0}^{i=\pi(n)-1} \frac{(-1)^i P^{(i)}(n)}{i!} x^i = 0 \end{cases}$$

### 3 Exemples

Traisons les exemples  $n = 8$  et  $n = 10$ . Il n'y a que trois nombres premiers impairs inférieurs à  $n$ , 3, 5 et 7. L'équation polynomiale  $(x - 3)(x - 5)(x - 7) = 0$  se développe en  $x^3 - 15x^2 + 71x - 105 = 0$ .

L'équation polynomiale portant sur  $n - x$  se développe quant à elle en :  
 $-x^3 + (3n - 15)x^2 + (-3n^2 + 30n - 71)x + (n^3 - 15n^2 + 71n - 105) = 0$ .

Si on remplace  $n$  par 8, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 15 = 0 \end{cases}$$

3 et 5 sont les seules solutions de ce système. Ce sont les décomposants de Goldbach de 8.

Si on remplace  $n$  par 10, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases}$$

Les deux équations sont équivalentes, 3 et 5 et 7 sont solutions de ce système, et sont décomposants de Goldbach de 10.

### 4 Démonstration graphique

On comprend aisément, puisque c'est ainsi qu'on les a construites, que les courbes des deux équations identifiées sont verticalement symétriques l'une de l'autre par rapport à un axe vertical d'équation  $x = n/2$ .

Imaginons deux points se déplaçant à même vitesse sur ces deux courbes, depuis le point d'ordonnée  $x = n/2$ , l'un vers la droite sur la première courbe, l'autre vers la gauche sur la deuxième courbe.

Premier cas, le point en question est sur l'axe des abscisses, il annule les deux courbes,  $n/2$  est un nombre premier ; un nombre pair double d'un nombre premier vérifie trivialement la conjecture.

Deuxième cas, le point en question n'annule pas les courbes, elles s'intersectent en lui, au-dessus ou bien au-dessous de l'axe des abscisses. Puis plusieurs fois, elles vont ainsi se croiser. A chaque fois qu'elles se croisent, les deux polynômes coïncident, n'en sont qu'un.

Prenons l'exemple du nombre pair 8 dont on a vu que les deux polynômes représentant ses décomposants de Goldbach sont les polynômes suivants :

$$\begin{aligned} x^3 - 15x^2 + 71x - 105 &= 0 \\ x^3 - 9x^2 + 23x - 15 &= 0 \end{aligned}$$

$n/2$  vaut 4. L'une des solutions de Goldbach est la solution 3 + 5, 3 et 5 sont séparés de 4, le milieu, par  $\Delta = 1$ . Voyons ce qu'il advient de nos deux polynômes lorsqu'on remplace  $x$  par  $x - 1$  dans le premier et  $x$  par  $x + 1$  dans le second.

$$\begin{aligned} (x + 1)^3 - 15(x + 1)^2 + 71(x + 1) - 105 &= x^3 - 12x^2 + 44x - 48 = 0 \\ (x - 1)^3 - 9(x - 1)^2 + 23(x - 1) - 15 &= x^3 - 12x^2 + 44x - 48 = 0 \end{aligned}$$

Si par contre on fait la même chose avec  $x - 3$  et  $x + 3$ , on n'obtient pas du tout les mêmes polynômes, ceci est dû au fait que 1 + 7 n'est pas une décomposition de Goldbach :

$$\begin{aligned} (x + 3)^3 - 15(x + 3)^2 + 71(x + 3) - 105 &= x^3 - 6x^2 + 8x = 0 \\ (x - 3)^3 - 9(x - 3)^2 + 23(x - 3) - 15 &= x^3 - 18x^2 + 104x - 192 = 0 \end{aligned}$$

Dans le cas du nombre pair 12 dont on sait que 5 + 7 est une décomposition située à un  $\Delta$  de 1 de la moitié de 12 qu'est 6, on obtient les transformations de polynômes suivantes avec Sage :

```
p = x^4 - 22 * x^3 + 164 * x^2 - 458 * x + 315
p.substitute(x = x - 1).expand()
>> x^4 - 26 * x^3 + 236 * x^2 - 856 * x + 960
p = x^4 - 26 * x^3 + 236 * x^2 - 886 * x + 1155
p.substitute(x = x + 1).expand()
>> x^4 - 22 * x^3 + 164 * x^2 - 488 * x + 480
```

Le polynôme obtenu par changement de variable dans le premier polynôme fournit un polynôme qui a le même début que le second polynôme et inversement, ce qui permet d'abaisser le degré des équations à résoudre. Malheureusement, on n'arrive pas du tout à obtenir des résultats semblables dès le degré 5.

C'est bien à cause de la Théorie de Galois que la conjecture de Goldbach est vraie : il y a un changement de la variable dans les deux polynômes par  $x - \Delta$  et  $x + \Delta$  qui fait que les deux polynômes n'en deviennent plus qu'un. Le changement en question fournit la décomposition de Goldbach du nombre pair considéré en  $(x - \Delta) + (x + \Delta)$ .

## Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 428, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

[3], **Léonard Euler**, *Démonstration sur le nombre de points où deux lignes des ordres quelconques peuvent se couper*, Mémoires de l'Académie des Sciences et belles lettres de Berlin [4], Berlin, 1750, p.234-248.

[4], **Léonard Euler**, *Nouvelle méthode d'éliminer les quantités inconnues des équations*, Mémoires de l'Académie des Sciences et belles lettres de Berlin [20], Berlin, 1764, p.91-104.

## Annexe 1 : exemples des degrés 2 à 6

Si on résout les équations dont on a calculé les coefficients en remplaçant  $n$  successivement par les valeurs 12 (équations de degré 4 car il y a 4 nombres premiers impairs inférieurs à 12 qui sont 3, 5, 7 et 11) puis par les valeurs 14 et 16 pour  $n$  (équations polynomiales de degré 5 car on a rajouté le nombre premier impair 13), et enfin 18 (degré 6) avec un outil tel que l'outil libre Sage qui permet la résolution d'équations polynomiales, on arrive à résoudre les systèmes ci-dessous.

Pour  $n = 12$ , il faut résoudre le système :

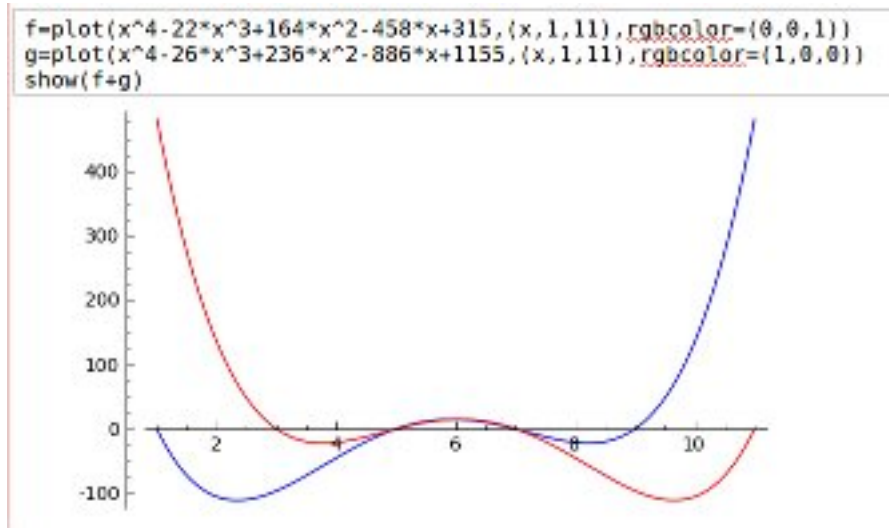
$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 + (26 - 4n)x^3 + (6n^2 - 78n + 236)x^2 + (-4n^3 + 78n^2 - 472n + 886)x + (n^4 - 26n^3 + 236n^2 - 886n + 1155) = 0 \end{cases}$$

qui se ramène au système :

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 - 22x^3 + 164x^2 - 458x + 315 = 0 \end{cases}$$

Les seules valeurs de  $x$  qui conviennent sont bien 5 et 7 qui sont bien les décomposants de Goldbach de 12.

La visualisation des deux polynômes par l'outil libre Sage est fournie ci-dessous :



Calculons les équations pour le degré 5 (nombres premiers impairs 3, 5, 7, 11 et 13).

$$x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 10725 = 0$$

avec

$$3 + 5 + 7 + 11 + 13 = 39$$

$$3.5 + 3.7 + 3.11 + 3.13 + 5.7 + 5.11 + 5.13 + 7.11 + 7.13 + 11.13 = 574$$

$$3.5.7 + 3.5.11 + 3.5.13 + 3.7.11 + 3.7.13 + 3.11.13 + 5.7.11 + 5.7.13 + 5.11.13 + 7.11.13 = 3954$$

$$3.5.7.11 + 3.5.7.13 + 3.5.11.13 + 3.7.11.13 + 5.7.11.13 = 12673$$

$$3.5.7.11.13 = 15015.$$

En remplaçant  $x$  par  $n - x$ , on obtient le polynôme suivant dont on cherche quelles valeurs de  $x$  l'annulent.

$$\begin{array}{rcccccc}
 & & & & & & -x^5 \\
 & & & & & + (5n & -39) & x^4 \\
 & & & + (-10n^2 & +156n & -574) & x^3 \\
 & + (10n^3 & -234n^2 & +1722n & -3954) & x^2 \\
 + (-5n^4 & +156n^3 & -1722n^2 & +7908n & -12673) & x^1 \\
 + (n^5 & -39n^4 & +574n^3 & -3954n^2 & +12673n & -15015)
 \end{array}$$

Pour  $n = 14$  ou  $n = 16$ , il faut résoudre le système :

$$\begin{cases}
 x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\
 -x^5 + (5n - 39)x^4 + (-10n^2 + 156n - 574)x^3 + (10n^3 - 234n^2 + 1722n - 3954)x^2 + \\
 (-5n^4 + 156n^3 - 1722n^2 + 7908n - 12673)x + (n^5 - 39n^4 + 574n^3 - 3954n^2 + 12673n - 15015) = 0
 \end{cases}$$

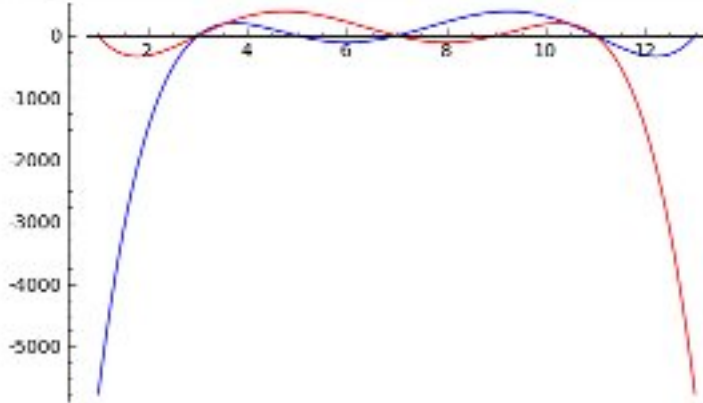
qui se ramène dans le cas de  $n = 14$  au système :

$$\begin{cases}
 x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\
 -x^5 + 31x^4 - 350x^3 + 1730x^2 - 3489x + 2079 = 0
 \end{cases}$$

Les seules valeurs de  $x$  qui conviennent sont 3, 7 et 11, qui sont bien les décomposants de Goldbach de 14.

La visualisation des deux polynômes par l'outil libre Sage est fournie ci-dessous :

```
f=plot(x^5-39*x^4+574*x^3-3954*x^2+12673*x-15015,(x,1,13),rgbcolor=(0,0,1))
g=plot(-x^5+31*x^4-350*x^3+1730*x^2-3489*x+2079,(x,1,13),rgbcolor=(1,0,0))
show(f+g)
```



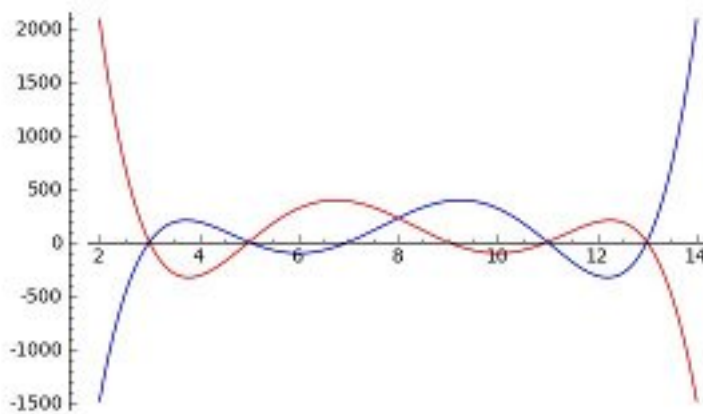
Pour  $n = 16$ , le système final à résoudre est :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 41x^4 - 638x^3 + 4654x^2 + 15681x - 19305 = 0 \end{cases}$$

Le pgcd de ces deux polynômes est  $x^4 - 32x^3 + 350x^2 - 1504x + 2145$ . Les seules valeurs de  $x$  qui conviennent sont 3, 5, 11 et 13, qui sont bien les décomposants de Goldbach de 16.

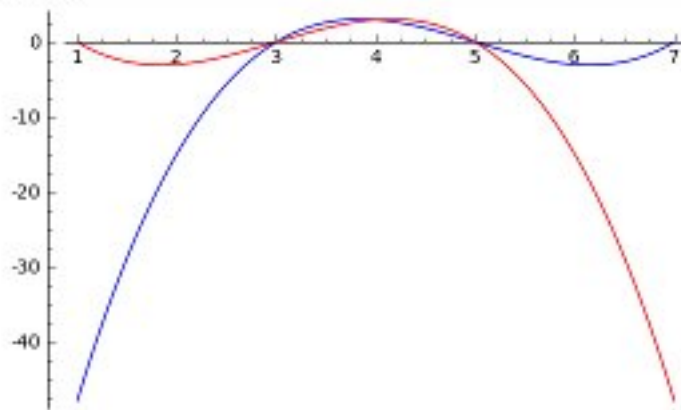
La visualisation des deux polynômes par l'outil libre Sage est fournie ci-dessous :

```
f=plot(x^5-39*x^4+574*x^3-3954*x^2+12673*x-15015,(x,2,14),rgbcolor=(0,0,1))
g=plot(-x^5+41*x^4-638*x^3+4654*x^2-15681*x+19305,(x,2,14),rgbcolor=(1,0,0))
show(f+g)
```

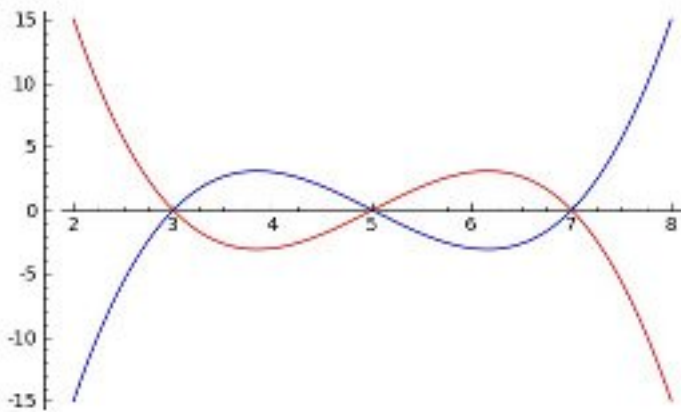


Fournissons enfin les visualisations par l'outil libre Sage des polynômes permettant de trouver les décomposants de Goldbach des nombres pairs 6, 8, 10 et 18.

```
f=plot(x^3-15*x^2+71*x-105,(x,1,7),rgbcolor=(0,0,1))
g=plot(-x^3+9*x^2-23*x+15,(x,1,7),rgbcolor=(1,0,0))
show(f+g)
```



```
f=plot(x^3-15*x^2+71*x-105,(x,2,8),rgbcolor=(0,0,1))
g=plot(-x^3+15*x^2-71*x+105,(x,2,8),rgbcolor=(1,0,0))
show(f+g)
```



```
f=plot(x^6-56*x^5+1237*x^4-13712*x^3+79891*x^2-230456*x+255255,(x,1,17),rgbcolor=(0,0,1))
g=plot(x^6-52*x^5+1057*x^4-10552*x^3+52891*x^2-118420*x+75075,(x,1,17),rgbcolor=(1,0,0))
show(f+g)
```

