Promenade modulaire

Nicolas Billerey

Lycée Blaise Pascal

Mardi 3 décembre 2019

Sommaire

Sommaire

Un petit calcul...

On calcule les produits

$$(1-x)(1-x^2) = 1 - x - x^2 + x^3$$
$$(1-x)(1-x^2)(1-x^3) = 1 - x - x^2 + x^4 + x^5 - x^6$$
$$(1-x)(1-x^2)(1-x^3)(1-x^4) = 1 - x - x^2 + x^4 + 2x^5 - x^8 - x^9 + x^{10}$$

. . .de plus en plus loin. . .

Que vaut $(1-x)(1-x^2)\cdots(1-x^n)$?

$$
\begin{array}{lllllllll}
(n=2) & 1-x-x^2+x^3 & & & & & & & \\
(n=3) & 1-x-x^2 & & +x^4+x^5-x^6 & & & & & \\
(n=4) & 1-x-x^2 & & +2x^5 & & -x^8-x^9+x^{10} & & & \\
(n=5) & 1-x-x^2 & & +x^5+x^6 & +x^7-x^8-x^9-x^{10}\ldots & & & & \\
(n=6) & 1-x-x^2 & & +x^5 & +2x^7 & -x^9-x^{10}\ldots & & & \\
(n=7) & 1-x-x^2 & & +x^5 & +x^7+x^8 & -x^{10}\ldots & & & \\
(n=8) & 1-x-x^2 & & +x^5 & +x^7 & +x^9 & \ldots & & \\
(n=9) & 1-x-x^2 & & +x^5 & +x^7 & & +x^{10}\ldots & & \\
(n=10) & 1-x-x^2 & & +x^5 & +x^7 & & & \ldots &
\end{array}
$$

- Les termes se stabilisent : le produit infini a donc un sens.
- Il y a beaucoup d'annulations : tous les coefficients valent -1, 0 ou 1.

. . .jusqu'à l'infini !

On obtient, formellement,

$$\Phi(x) = \prod_{n=1}^{\infty}(1-x^n) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + x^{51} + x^{57} - x^{70} - x^{77} \dots$$

- Il y a beaucoup de zéros (et quelques signes $-$ et $+$).
- On a toujours deux signes $-$ suivis de deux signes $+$.
- Les degrés des termes non nuls sont

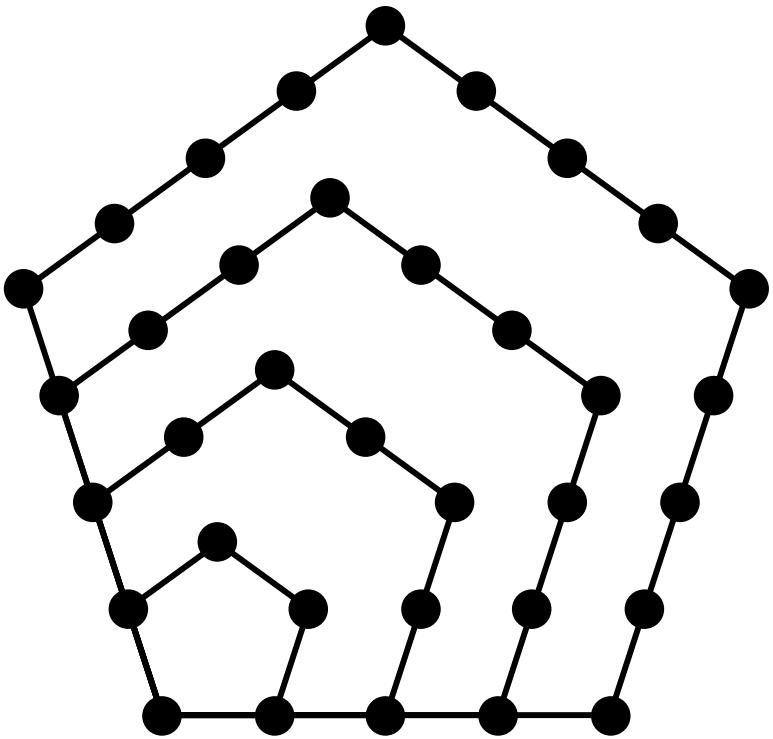
$$0,\ 1,\ 2,\ 5,\ 7,\ 12,\ 15,\ 22,\ 26,\ 35,\ 40,\ 51,\ 57,\ 70,\ 77, \dots$$

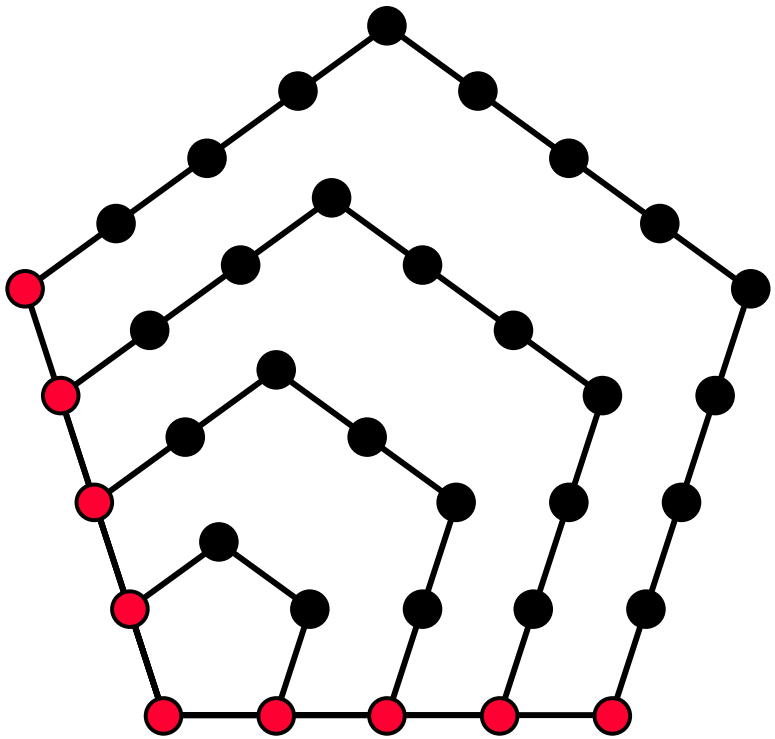
Ça vous dit quelque chose ? Pas évident. . .

Nombres pentagonaux

0, 1, 2, 5, 7, 12, 15, 22, 26, 35, 40, 51, 57, 70, 77, ... est la suite A001318 de l'On-line Encyclopedia of Integer Sequences, celle des *nombres pentagonaux généralisés* :

$$\frac{3n^2 - n}{2}, \quad n = 0,\ 1,\ -1,\ 2,\ -2,\ 3,\ -3, \ldots$$





Théorème des nombres pentagonaux (Euler, 1707-1783) :

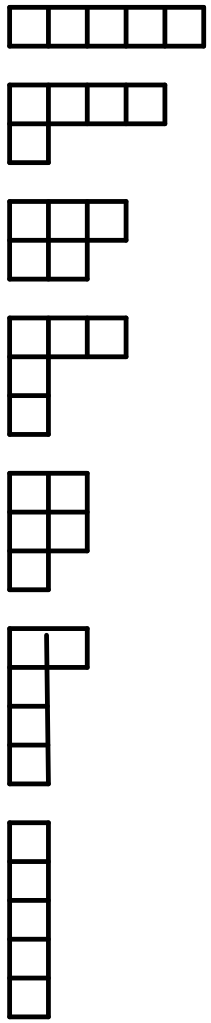
$$\prod_{n=1}^{+\infty}(1-x^n) = \sum_{-\infty}^{+\infty}(-1)^n x^{\frac{3n^2-n}{2}}.$$

Fonction de partition

On note $p(n)$ le nombre de façons (à l'ordre près) d'écrire un entier $n \geq 1$ comme somme d'entiers naturels non nuls.

$$
\begin{aligned}
5 &= 5 \\
&= 4+1 \\
&= 3+2 \\
&= 3+1+1 \\
&= 2+2+1 \\
&= 2+1+1+1 \\
&= 1+1+1+1+1
\end{aligned}
$$

$$p(5) = 7$$



De la fonction de partition à la fonction Φ d'Euler

On pose

$$P(x) = 1 + \sum_{n=1}^{\infty} p(n)x^n = 1 + x + 2x^2 + 3x^3 + 5x^4 + 7x^5 + 11x^6 \cdots$$

On vérifie que l'on a

$$\Phi(x)P(x) = 1.$$

Le théorème des nombres pentagonaux fournit alors la formule de récurrence (où $p(k) = 0$ si $k < 0$ et $p(0) = 1$) :

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) \cdots$$

Ainsi, on a par exemple

$$\begin{aligned} p(8) &= p(7) + p(6) - p(3) - p(1) \\ &= 3p(5) + 2p(4) - p(3) - p(2) - 3p(1) - p(0) \\ &= 3 \times 7 + 2 \times 5 - 3 - 2 - 3 \times 1 - 1 = 22 \end{aligned}$$

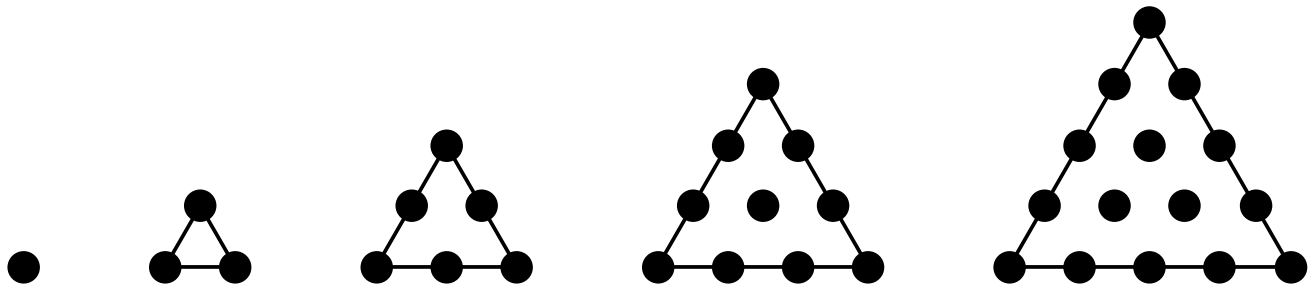
Φ au cube, joue-la comme Gauss

$$\Phi(x)^3 = \prod_{n=1}^{\infty}(1-x^n)^3 = 1 - 3x + 5x^3 - 7x^6 + 9x^{10} - 11x^{15} + 13x^{21} \cdots$$

- Il y a beaucoup de zéros.
- Les coefficients sont des nombres impairs avec des signes qui alternent.
- Les degrés des termes non nuls sont

$$0,\ 1,\ 3,\ 6,\ 10,\ 15,\ 21, \ldots$$

Ce sont les nombres de la forme $\frac{n(n+1)}{2}$ $(n = 0, 1, 2, 3, \ldots)$. On les appelle *nombres triangulaires*.



Φ au cube, et après ?

Théorème (Gauss, 1777–1855) :

$$\Phi(x)^3 = \prod_{n=1}^{\infty}(1-x^n)^3 = \sum_{n=0}^{\infty}(-1)^n(2n+1)x^{\frac{n(n+1)}{2}}.$$

- Pour certaines valeurs de d, MacDonald a donné (1972) des formules pour Φ^d.
- Ses résultats sont reliés à la théorie des algèbres de Lie.

Pour $d = 24$

Ramanujan (1887–1920) a étudié en détail la fonction $\Phi(x)^{24}$.

$$\begin{aligned}\Phi(x)^{24} &= 1 - 24x + 252x^2 - 1472x^3 + 4830x^4 - 6048x^5 \cdots \\ &= \sum_{n=1}^{\infty} \tau(n) x^{n-1}.\end{aligned}$$

La fonction τ : Dark Side

n	1	2	3	4	5	6	7	8
$\tau(n)$	1	-24	252	-1472	4830	-6048	-16744	84480

Les propriétés des nombres $\tau(n)$ aussi riches que mystérieuses :

- Lehmer a conjecturé en 1947 que $\tau(n)$ n'est jamais nul ; cela a été vérifié pour tout $n \leq 227982415202426879 99 \simeq 2,3 \cdot 10^{19}$ (Bosman, 2007), mais on n'a pas de preuve !
- On conjecture qu'il existe une infinité de nombres premiers p pour lesquels p divise $\tau(p)$ mais on n'en connaît que six :

$$2,\ 3,\ 5,\ 7,\ 2411,\ 775833763$$

et il n'y en a pas d'autre avant 10^{10} (Lygeros et Rozier, 2010) !

La fonction τ : Light Side

n	1	2	3	4	5	6	7	8
$\tau(n)$	1	-24	252	-1472	4830	-6048	-16744	84480

$$\begin{aligned}\tau(6) &= -6048\\ &= -24 \times 252\\ &= \tau(2) \times \tau(3)\end{aligned}$$

$$\begin{aligned}\tau(4) &= -1472\\ &= 576 - 2048\\ &= \tau(2)^2 - 2^{11}\tau(1)\end{aligned}$$

$$\begin{aligned}\tau(8) &= 84480\\ &= 35328 + 49152\\ &= \tau(4)\tau(2) - 2^{11}\tau(2)\end{aligned}$$

La fonction τ : Light Side

En 1916, Ramanujan a conjecturé les relations suivantes :

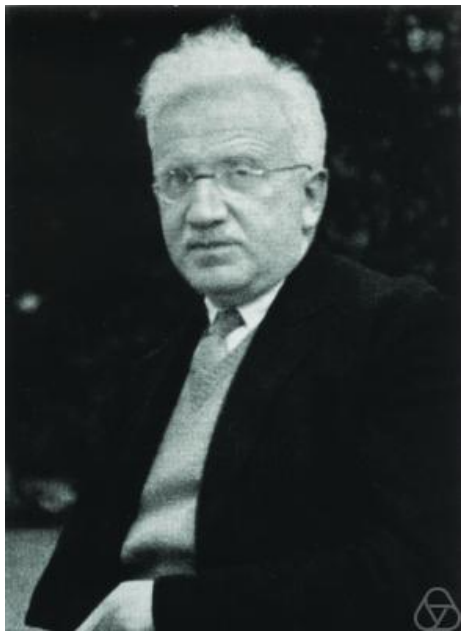
1. si n et m sont premiers entre eux, alors $\tau(nm) = \tau(n)\tau(m)$;
2. si p est un nombre premier et n un entier ≥ 2, alors

$$\tau(p^n) = \tau(p)\tau(p^{n-1}) - p^{11}\tau(p^{n-2}) ;$$

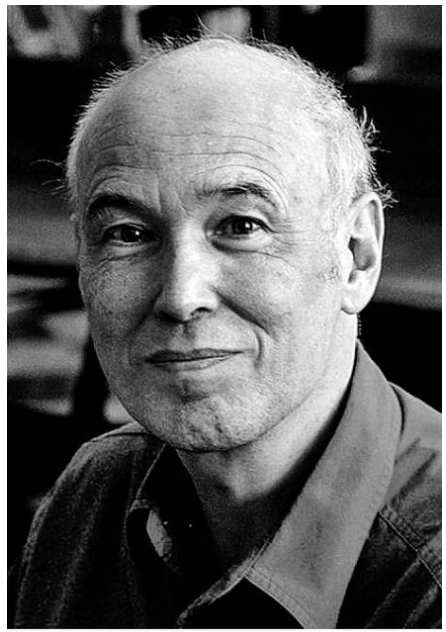
3. si p est un nombre premier, alors $|\tau(p)| \leq 2p^{\frac{11}{2}}$.

La fonction τ : Light Side

- Les deux premières relations ont été démontrées par Mordell en 1917, puis par Hecke en 1930 ;
- La dernière est une conséquence de résultats *très* généraux de Deligne pour lesquels il a reçu la médaille Fields en 1978.



Hecke (1887–1947)

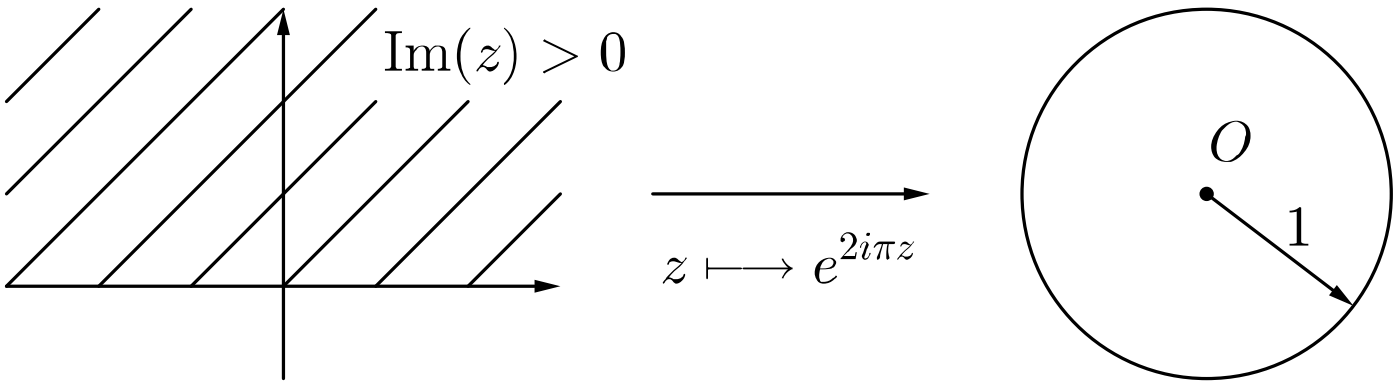


Deligne (1944–)

La fonction τ et la forme modulaire Δ

Définition

Pour $z \in \mathbb{C}$ avec $\mathrm{Im}(z) > 0$, on pose $q = e^{2i\pi z}$.



Toutes les relations précédentes sont liées au fait que la fonction

$$\Delta(z) = q\Phi(q)^{24} = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q + \sum_{n=1}^{\infty}\tau(n)q^n$$

est une *forme modulaire*.

Sommaire

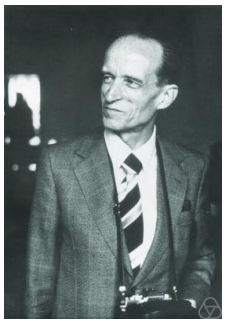
Les formes modulaires sont partout !

Il y a cinq opérations fondamentales en mathématiques : l'addition, la soustraction, la multiplication, la division et les formes modulaires.

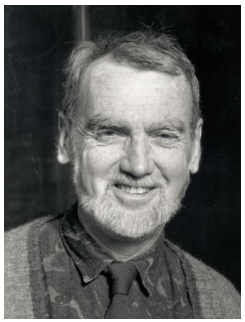
— (attribué à) Martin Eichler (1912–1992)

Les formes modulaires interviennent de façon cruciale dans

- le programme de Langlands (1967) ;
- la démonstration du « dernier théorème de Fermat » (Wiles, 1995) ;
- le problème des empilements de sphères (Viazovska, 2016) ;
- etc.







L'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$

Le groupe

$$\mathrm{SL}_2(\mathbb{Z}) = \{\gamma \in \mathrm{M}_2(\mathbb{Z}) \mid \det(\gamma) = 1\}$$

agit sur le demi-plan de Poincaré

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

par homographies

$$\left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \in \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} \longmapsto \gamma \cdot z = \frac{az+b}{cz+d} \in \mathbb{H}$$

Exemples

- La matrice $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ agit par translation $z \mapsto z+1$.
- La matrice $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ agit par inversion $z \mapsto -\frac{1}{z}$.

Fonctions invariantes

L'espace

$$M_0(1) = \{f : \mathbb{H} \to \mathbb{C} \text{ holomorphe sur } \mathbb{H} \cup \{\infty\} \text{ telle que } f(\gamma \cdot z) = f(z), \text{ pour tout } \gamma \in \mathrm{SL}_2(\mathbb{Z}) \text{ et tout } z \in \mathbb{H}\}$$

des fonctions invariantes sous cette action est réduit aux constantes...

Soit $N \geq 1$ et $k \geq 2$ deux entiers. On définit

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\} \leq \mathrm{SL}_2(\mathbb{Z})$$

et pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et $z \in \mathbb{H}$, on pose

$$j(\gamma, z) = cz + d.$$

Formes modulaires

On définit alors l'espace des formes de *niveau* N et *poids* k :

$$M_k(N) = \Big\{ f : \mathbb{H} \to \mathbb{C} \text{ holomorphe sur } \mathbb{H} \cup \{\infty\} \text{ telle que } f(\gamma \cdot z) = j(\gamma, z)^k f(z), \text{ pour tout } \gamma \in \Gamma_0(N) \text{ et tout } z \in \mathbb{H} \Big\}.$$

C'est un $\mathbb{C}$-espace vectoriel de dimension finie !

Exemples

- La fonction $\Delta(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24}$ appartient à $M_{12}(1)$. En particulier, on a $\Delta\left(-\frac{1}{z}\right) = z^{12}\Delta(z)$ et $\Delta(z+1) = \Delta(z)$.
- Pour tout $k \geq 4$ pair, on a $G_k(z) = \sum_{(n,m)\neq(0,0)} \frac{1}{(m+nz)^k} \in M_k(1)$.
- Une base de l'espace vectoriel $M_{12}(1)$ est $(\Delta,\ G_{12})$.

Développement de Fourier

Toute forme modulaire f est invariante par l'action de $T : z \mapsto z + 1$. En particulier, elle s'écrit

$$f(z) = a_0 + a_1 q + a_2 q^2 + a_3 q^3 + \cdots = \sum_{n=0}^{\infty} a_n q^n$$

où, sous de bonnes hypothèses, les coefficients (de Fourier) $\{a_n\}_{n \geq 1}$ sont des *entiers* (algébriques).

Exemples

- On a $\Delta(z) = q + \sum_{n \geq 1} \tau(n) q^n \in \mathbb{Z}[[q]]$.
- Pour tout $k \geq 4$ pair, on a

$$G_k(z) = 2 \cdot \frac{(2i\pi)^k}{(k-1)!} \left(-\frac{B_k}{2k} + \sum_{n \geq 1} \left(\sum_{d|n} d^{k-1} \right) q^n \right),$$

où B_k est le k-ième nombre de Bernoulli.

Sommaire

Courbes elliptiques

Une *courbe elliptique* est une courbe plane donnée par une équation de la forme

$$y^2 = g(x),$$

avec $g \in \mathbb{Z}[X]$ unitaire, $\deg(g) = 3$ et g sans racine multiple.

1. Quelle est la structure/forme de l'ensemble des solutions de cette équation dans $\mathbb{C}$? dans $\mathbb{R}$? dans $\mathbb{Q}$? dans $\mathbb{Z}/p\mathbb{Z}$ (avec p premier) ?
2. Combien y en a-t-il ?

Un exemple concret : la courbe d'équation $y^2 = x^3 - x + 1$

- Combien a-t-elle de solutions modulo 3 ?

x	0	1	2
$x^3 - x + 1$	1	1	1
$\#y$	2	2	2

Il y a 6 solutions modulo 3.

- Combien a-t-elle de solutions modulo 5 ?

x	0	1	2	3	4
$x^3 - x + 1$	1	1	2	0	1
$\#y$	2	2	0	1	2

Il y a 7 solutions modulo 5.

Modularité des courbes elliptiques

Théorème (Wiles et al.)

Soit $E : y^2 = g(x)$ une courbe elliptique. Il existe une forme modulaire $f_E = \sum_{n \geq 1} a_n q^n$ de poids 2 et d'un certain niveau N_E (le conducteur de E) telle que

$$a_p = p - \#\left\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \text{ tel que } y^2 \equiv g(x) \pmod{p}\right\}$$

pour tout nombre premier p, sauf un nombre fini.

Exemple

La forme modulaire f_E associée à la courbe elliptique $E : y^2 = x^3 - x + 1$ est de poids 2 et de niveau $92 = 2^2 \cdot 23$:

$$f_E = q - 3q^3 - 2q^5 - 4q^7 + 6q^9 + 2q^{11} - 5q^{13} + \cdots$$

Du théorème de Wiles à l'équation de Fermat

Soit $\ell \geq 5$ un nombre premier et soit a, b, c trois entiers non nuls premiers entre eux tels que

$$a^\ell + b^\ell = c^\ell.$$

- L'équation $y^2 = x(x - a^\ell)(x + b^\ell)$ définie une courbe elliptique E appelée *courbe de Hellegouarch-Frey*.
- La forme modulaire associée par Wiles à E est de poids 2 et de niveau N_E *dépendant de* E (et donc de a, b et c).
- Par des théorèmes (difficiles !) de Mazur (1977) et Ribet (1990), la forme f_E est « congrue modulo ℓ » à une forme $g = \sum_{n \geq 1} b_n q^n$ de poids 2 et de niveau 2 (i.e. $a_p - b_p$ est « divisible » par p pour tout nombre premier p sauf un nombre fini).
- Or il n'existe pas de forme modulaire (non nulle) de poids 2 et de niveau 2 ! CQFD

Merci pour votre attention !