De Gauss à la théorie des nombres moderne

Exposé au CPPM
Marseille Luminy
le 8 décembre 2012

Guy Henniart
Département de Mathématiques
Université Paris-Sud
Laboratoire de Mathématiques
d'Orsay, UMR 8628 du CNRS
Institut Universitaire de France

Nombres entiers, nombres premiers

$1, 2, 3, 4 = 2 \times 2 = 2^2, 5$

$6 = 2 \times 3, 7, 8 = 2 \times 2 \times 2 = 2^3,$

$9 = 3 \times 3 = 3^2, 10 = 2 \times 5, 11,$

$12 = 2 \times 2 \times 3 = 2^2 \times 3, 13,$ etc.

→ nombres composés, nombres premiers

- Tout nombre composé est produit de nombres premiers. Deux décompositions d'un nombre composé comme produit de nombres premiers ne diffèrent que par l'ordre des facteurs

$12 = 2 \times 2 \times 3 = 2 \times 3 \times 2 = 3 \times 2 \times 2$

L'équation de Fermat

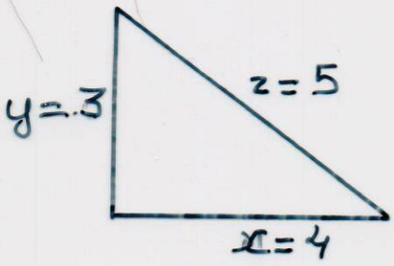
r est un entier fixé $r \geqslant 3$

On cherche les solutions en entiers $\geqslant 1$ de l'équation

$$X^r + Y^r = Z^r$$

Théorème (A. Wiles, R. Taylor et A. Wiles ≃1994) Cette équation n'a pas de solutions en entiers $\geqslant 1$.

Le cas où r vaut 2 : triangles pythagoriciens



$$4^2 + 3^2 = 5^2$$

$$16 + 9 = 25$$

Quels sont les triangles rectangles dont les côtés x et y et l'hypoténuse z sont entiers ?

Identités remarquables :

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$(a-b)^2 = a^2 - 2ab + b^2$$

d'où $(a+b)^2 = (a-b)^2 + 4ab$

Si $a = m^2$ et $b = n^2$,

on a la solution

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2$$

→ Toutes les solutions en entiers ≥ 1

$$x = k(m^2 - n^2), \quad y = 2kmn, \quad z = k(m^2 + n^2)$$

ou

$$x = 2kmn, \quad y = k(m^2 - n^2), \quad z = k(m^2 + n^2)$$

(ici $m > n \geq 1$, $k \geq 1$).

Wiles : pour $r \geq 3$, pas de solution à $X^r + Y^r = Z^r$ donnée par de telles formules, mais pas de solution « isolée » non plus !

Un bref historique

Fermat (1605? - 1665)

$r = 4$

Remarque : il suffit de traiter le cas où r est premier impair :
si $X^{rs} + Y^{rs} = Z^{rs}$ alors $(X^s)^r + (Y^s)^r = (Z^s)^r$.

Euler (1707 - 1783) $r = 3$

Legendre, Dirichlet $\simeq$ 1825 $r = 5$

Lamé 1839 $r = 7$

Kummer 1846 : $r \leq 100$ sauf quelques exceptions
méthode : nombres entiers « cyclotomiques »
mais factorisation non unique

$\simeq$ 1970 $r \leq 125\,000$

années 80 : passer par les congruences et utiliser le lien avec des fonctions spéciales, les formes modulaires du 19ème siècle

Congruences

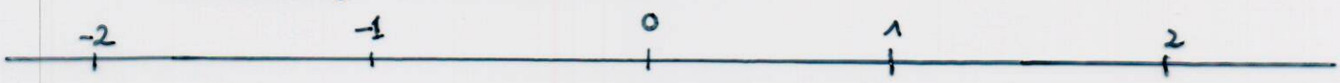
$N \geq 2$

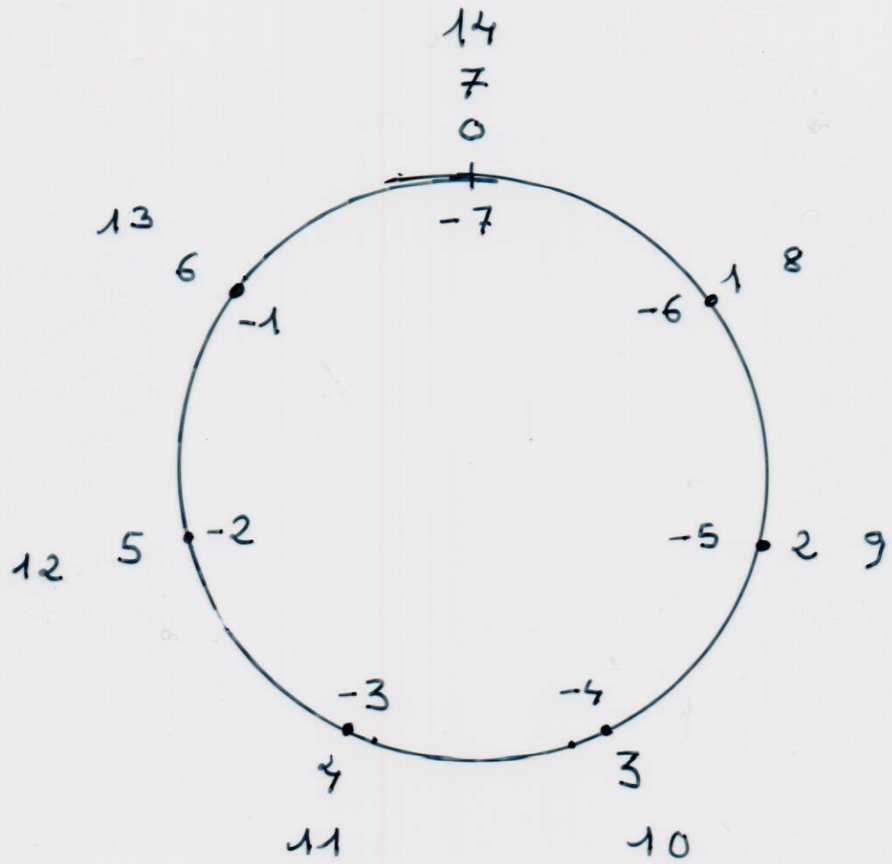
Deux entiers a, b sont <u>congrus modulo N</u> $a \equiv b \pmod{N}$ si $a - b$ est un multiple de N

<u>Exemples</u> 1) $a \equiv b \pmod{2}$ quand a et b sont tous deux pairs ou tous deux impairs

2) $a \equiv b \pmod{10}$ quand a et b ont même chiffre des unités

3) « preuve par 9 » : congruences modulo $9 = 10 - 1$.





On garde les trois opérations

$a \bmod N + b \bmod N = (a+b) \bmod N$

$a \bmod N - b \bmod N = (a-b) \bmod N$

$a \bmod N \times b \bmod N = ab \bmod N$

Exemples : $3 \bmod 7 + 5 \bmod 7 = 1 \bmod 7$

$3 \bmod 7 - 5 \bmod 7 = 5 \bmod 7$

$3 \bmod 7 \times 5 \bmod 7 = 1 \bmod 7$

$2 \bmod 7 \times 4 \bmod 7 = 1 \bmod 7$

Quand N est premier, on a la quatrième opération, la division exacte (mais pas par $0 \bmod N$!)

Exemples $1 \bmod 7 / 5 \bmod 7 = 3 \bmod 7$

$3 \bmod 7 / 4 \bmod 7 = 6 \bmod 7$

$2 \bmod 6 \times 3 \bmod 6 = 0 \bmod 6$

on ne peut diviser $3 \bmod 6$ par $2 \bmod 6$

→ On peut considérer des équations en « entiers modulo N ».

Gauss et la loi de réciprocité quadratique.

n un entier ≥ 2, sans facteurs carrés

$n = 3$ par exemple

Pour p premier, $3 \bmod p$ est-il le carré d'un entier modulo p ?

exemple : $p = 7$: non !

$p = 11$ oui : $(5 \bmod 11)^2 = 25 \bmod 11 = 3 \bmod 11$

Problème : pour p un nombre premier variable, peut-on prédire le nombre de solutions en entiers modulo p de l'équation

$$X^2 = n \bmod p \ ?$$

Réponse : oui, la réponse ne dépend que de $p \bmod 4n$

Exemple $n = 3$

p	2	3	5	7	11	13	17	19	23	29	31
N_p	1	1	0	0	2	2	0	0	2	0	0

Ce n'est pas général : si P est un polynôme à coefficients entiers, le nombre de solutions en entiers modulo p de l'équation

$$P \bmod p\,(X) = 0 \bmod p$$

ne dépend pas uniquement, quand p varie, de congruences en p.

Y-a-t-il des « lois » plus compliquées ?

Cas des courbes

Equations en 2 variables X et Y (courbes)

droites : $a.X + b\,Y = c$ $\quad a, b, c$ entiers

→ solutions en entiers modulo p de

$$(a \bmod p)X + (b \bmod p)\,Y = c \bmod p$$

toujours p pour p assez grand

coniques $a X^2 + bXY + cY^2 + dX + eY + f = 0$

(entiers $a, \dots, f$, conique propre)

nbre de solutions en entiers modulo p, pour p assez grand $= p$ + une erreur dépendant de congruences en p.

cubiques courbes elliptiques

$$Y^2 + aY = X^3 + bX^2 + cX + d \qquad a, b, c, d \text{ entiers}$$

N_p = nombre de solutions en entiers modulo p

$= p - a_p \qquad |a_p| \leq 2\sqrt{p}$

mais a_p ne dépend pas seulement de congruences en p !

Exemple (Eichler 1939)

$$Y^2 + Y = X^3 - X^2$$

p	2	3	5	7	11	13	17	19
$p - N_p$	-2	-1	1	-2	1	4	-2	0

Considérons l'expression

$$q(1-q)^2(1-q^{11})^2(1-q^2)^2(1-q^{22})^2(1-q^3)^2(1-q^{33})^2 \dots$$

et développons-la $\sum_{n \geq 1} a_n q^n$

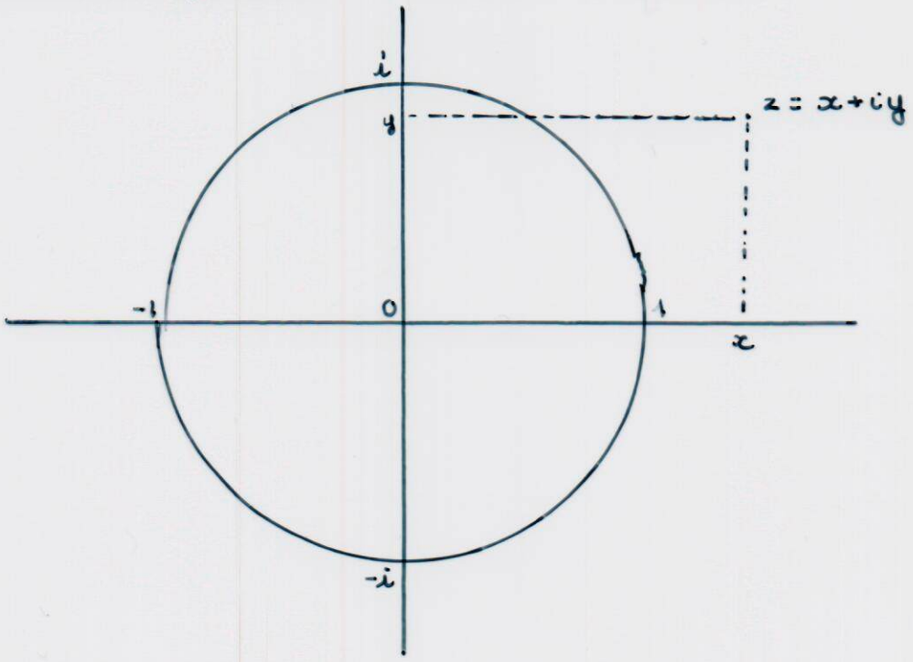
Alors pour p premier $\neq 11$ $\quad p - N_p = a_p$.

Interlude : nombres complexes

Nombres réels : $0,\ 1,\ -1,\ 1/3,\ \sqrt{2},\ \pi = 3{,}1415926\ldots$

→ droite réelle

Nombres complexes : plan complexe $\mathbb{C}$



4 opérations $(x+iy) \pm (x'+iy') = (x \pm x') + i(y \pm y')$

$(x+iy)(x'+iy') = (xx' - yy') + i(xy' + yx')$

en particulier $i^2 = -1$

$$\frac{1}{x+iy} = \frac{x-iy}{x^2+y^2} \qquad (\text{si } x \neq 0 \text{ ou } y \neq 0)$$

exponentielle complexe

$z = x+iy$ $\qquad e^z = e^x(\cos(y) + i\sin(y))$

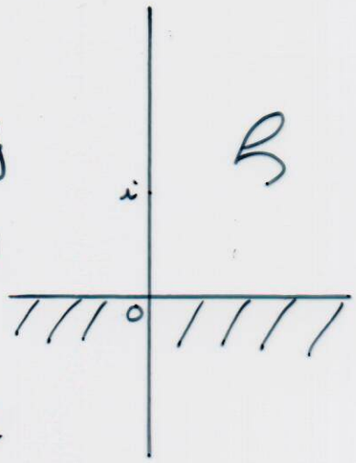
(nombre complexe non nul)

$e^{z+z'} = e^z \times e^{z'}$

Formes modulaires

fonctions $f : \mathcal{H} \to \mathbb{C}$

$\mathcal{H} = \{ z = x+iy \mid y > 0 \}$



f dérivable (au sens complexe)

$z \in \mathcal{G}$ $f(z+\underbrace{h}_{\text{petite variation}}) = f(z) + Ah + \underbrace{\text{erreur}}_{\substack{\text{négligeable} \\ \text{devant } h}}$

+ condition de croissance

+ équations fonctionnelles

• <u>niveau 1</u> et poids k (pair) ≥ 2

$$\begin{cases} f(z+1) = f(z) & (1) \\ f(-1/z) = z^k f(z) & (2) \end{cases}$$

Par (1) $f(z) = F(q) = \sum_{n \geq 0} a_n q^n$ $\quad q = e^{2\pi i z} = e^{-2\pi y}(\cos 2\pi x + i \sin 2\pi x)$

Par (1) et (2) on a

(3) $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ pour a, b, c, d entiers $ad - bc = 1$

<u>exemples</u> k pair ≥ 4 série d'Eisenstein

$G_k(z) = \alpha_k + \sum_{n \geq 1} \sigma_{k-1}(n) q^n$ $\quad (\alpha_k \neq 0$, calculé)

où $\sigma_s(n)$ = somme des puissances $s$èmes des diviseurs de n

f parabolique : $a_0 = 0$

<u>exemple</u> $k \leq 10$ pas de parabolique de niveau 1

$k = 12$ $\Delta(z) = q(1-q)^{24}(1-q^2)^{24}(1-q^3)^{24} \dots$

• <u>niveau</u> $N \geq 1$ et poids $k \geq 2$

On demande (3_N) $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ pour a, b, c, d entiers $ad - bc = 1$, c <u>multiple de</u> N

<u>exemples</u> $k = 2$ $N \leq 10$ pas de parabolique

$N = 11$ $\quad q(1-q)^2(1-q^{11})^2(1-q^2)^2(1-q^{22})^2(1-q^3)^2(1-q^{33})^2 \dots$

Les travaux de Wiles et autres

On part d'une courbe elliptique

$$Y^2 + aY = X^3 + bX^2 + cX + d \qquad a, b, c, d \text{ entiers}$$

et pour chaque entier premier p, on regarde le nombre N_p de solutions en entiers modulo p.

Alors il existe un entier $N \geq 1$ et une forme modulaire parabolique de poids 2 et niveau N

$$f(z) = \sum_{n \geq 1} a_n q^n$$

telle que $a_1 = 1$ et $a_p = p - N_p$ pour p ne divisant pas N

Application à l'équation de Fermat

solution hypothétique $A^r + B^r = C^r$ (r premier ≥ 3)

→ Courbe elliptique $Y^2 = X(X - A^r)(X + B^r)$ (Hellegouarc'h, G. Frey)

→ forme modulaire f de poids 2 et niveau N = produit des nombres premiers divisant A, B ou C.

mais cette forme f est trop belle pour exister : à cause de la puissance r dans les coefficients A^r, B^r, on a (K. Ribet) : écrivons $N = \ell M$ où ℓ est un nombre premier impair. Alors il existe une forme modulaire parabolique $g = \sum_{n \geq} b_n q^n$ de poids et niveau M telle que $b_1 = 1$ et que pour p premier ne divisant pas Nr, on ait

$$a_p \equiv b_p \text{ modulo } r.$$

On peut recommencer, en enlevant tous les nombres premiers impairs du niveau N, et on tombe sur une forme parabolique non nulle de poids 2 et de niveau 2, qui n'existe pas.