Formes modulaires et équations Diophantiennes

Colloquium

Jussieu.
Paris
Juin 2004

L'équation de Pell

L'équation "préférée" de Fermat?

$$\boxed{x^2 - dy^2 = 1.}$$

Loi de groupe:

$$(x_1, y_1) \star (x_2, y_2) := (x_1 x_2 + d y_1 y_2, x_1 y_2 + y_1 x_2).$$

Solution fondamentale: $(\pm x, \pm y) = (x_0, y_0)^{\star k}$.

1. Quelle peut être la taille de (x_0, y_0)?

2. Peut-on calculer (x_0, y_0) de manière *efficace*?

Quelques exemples

$d = 2$. $x = 3$, $y = 2$.

$d = 61$.
$x = 1766319049$,
$y = 226153980$.

$d = 109$.
$x = 158070671986249$,
$y = 15140424455100$.

$d = 991$.
$x = 379516400906811930638014896080$,
$y = 12055735790331359447442538767$.

Algorithmes

On dispose d'un très bon algorithme pour calculer (x_0, y_0):

L'algorithme de Fermat, basé sur les *fractions continues*.

$$\sqrt{d} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

$$\frac{p_n}{q_n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_n}}}.$$

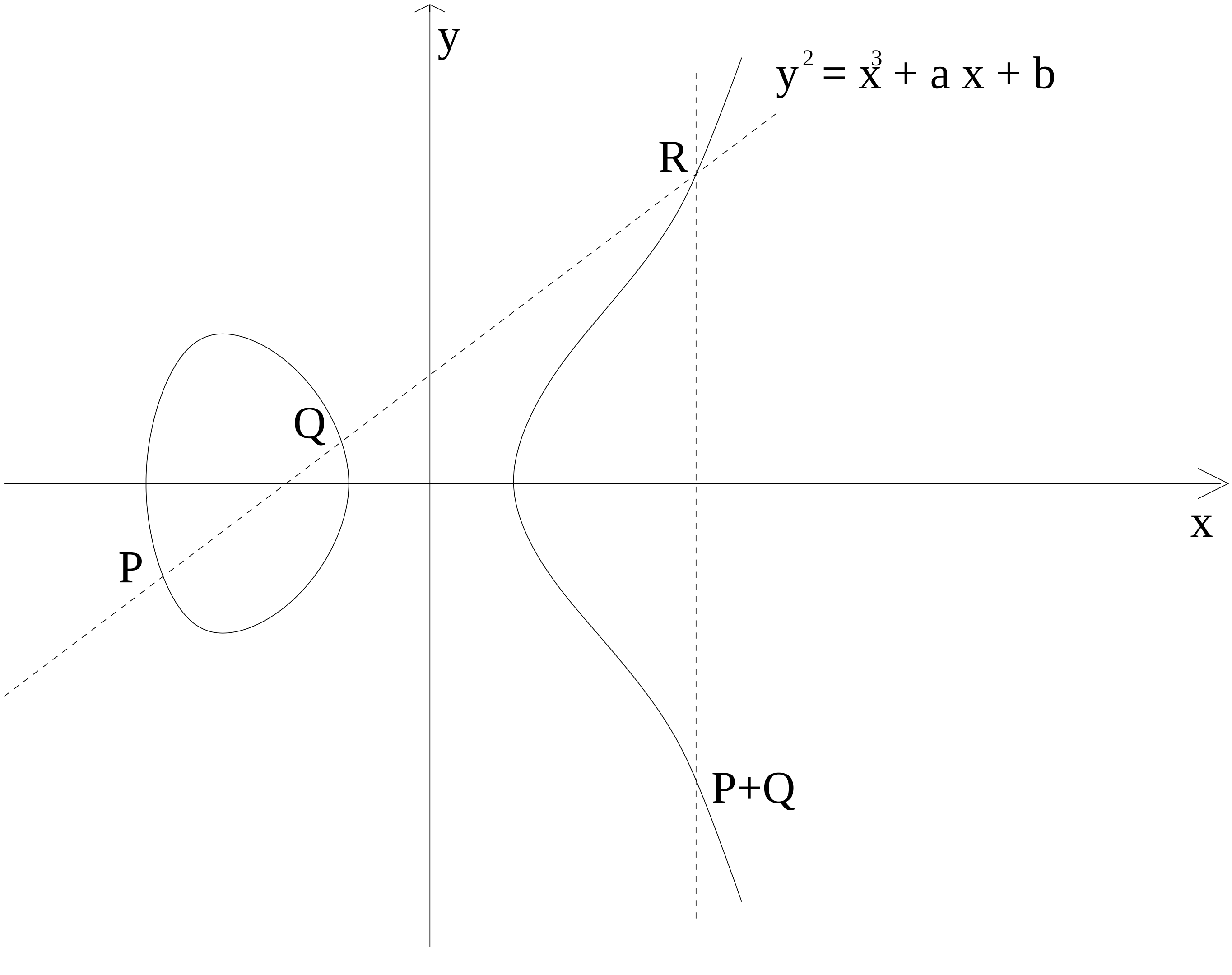
Pour un certain $n >> 0$, $(p_n, q_n) = (x_0, y_0)$.

Le calcul de (x_0, y_0) exige $O(\log(x_0))$ opérations.

$\log x_0$ étant un indicateur naturel de la taille du problème, l'algorithme de Fermat jouit d'une complexité *polynomiale*.

Courbes elliptiques

$$E : y^2 = x^3 + ax + b.$$



La loi d'addition sur une courbe elliptique

Le théorème de Mordell-Weil

Théorème. Le groupe $E(\mathbf{Q})$ est un groupe abélien de *type fini*.

$$E(\mathbf{Q}) = T \oplus \mathbf{Z}^r, \quad r \geq 0.$$

Question. Y a-t-il un algorithme (polynomial??) pour calculer $E(\mathbf{Q})$ étant donné E?

On ne connait pas la réponse! (Cette question est liée à la conjecture de Shafarevich-Tate, et à celle de Birch et Swinnerton-Dyer.)

Une question (un peu) plus abordable

Question. Etant donné (E, M), avec $M \in \mathbf{R}^{>0}$, trouver un point non-trivial de $E(\mathbf{Q})$ de hauteur logarithmique $\leq M$, si un tel point existe, ou dire qu'un tel point n'existe pas, si tel est le cas.

Algorithme Evident: Parcourir tous les x tels que $ht(x) < M$.

Complexité: Exponentielle!

Un exemple de Bremner et Cassels

La courbe elliptique

$$E : y^2 = x^3 + 877x$$

est de rang un, engendré par (x, y) où:

$$x = \frac{612776083187947368101^2}{7884153586068390021 0^2}$$

$$y = \frac{\begin{array}{r}256256267988926809388 77\\ 68340455130896486691\\ 53204356603464786949\end{array}}{78841535860683900210^3}$$

Modularité

N :=Conducteur(E).

On pose:

$$a_p := \begin{cases} p+1-\#E(\mathbf{Z}/p\mathbf{Z}) & \text{si } p \not| N; \\ 0, 1, \text{ ou } -1 & \text{si } p|N. \end{cases}$$

$$a_{p^n} = a_p a_{p^{n-1}} - p a_{p^{n-2}},$$

$$a_{rs} := a_r a_s, \quad (r,s) = 1.$$

Problème: Y a-t-il une "formule explicite" pour les a_n?

On considère la série génératrice:

$$f_E(q) := \sum_{n=1}^{\infty} a_n q^n, \quad q := e^{2\pi i \tau}.$$

Formes Modulaires

Le sous-groupe de congruence de Hecke:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z}) \quad \text{s.t. } N|c \right\}.$$

Il agit sur $\mathcal{H} := \{z \in \mathbf{C} \text{ s.t. } \Im(z) > 0\}$ (demi-plan de Poincaré.)

Définition. Une *forme modulaire* de poids k et de niveau N est une fonction holomorphe sur $\mathcal{H}$

$$f(z) = \sum_{n=0}^{\infty} b_n e^{2\pi i n z}$$

telle que

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z),$$

$$\text{pour tout } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Le Théorème de Wiles

Théorème (Wiles) La série génératrice $f_E(z)$ est une forme modulaire de poids 2 et de niveau N.

Enoncé complémentaire: Soit

$$\exp_E : \mathbf{C} \longrightarrow E(\mathbf{C})$$

l'exponentielle de Lie. Il existe $\lambda \in \mathbf{C}^\times$ tel que

$$\Phi(\tau) := \exp_E \left(\lambda \int_{i\infty}^{\tau} f_E(z) dz \right)$$

donne une application bien définie:

$$\boxed{\Phi : \mathcal{H}/\Gamma_0(N) \longrightarrow E(\mathbf{C}),}$$

appelée *paramétrisation modulaire*.

Multiplication Complexe

Soit $K = \mathbf{Q}(\sqrt{-D}) \subset \mathbf{C}$ un *corps quadratique imaginaire*.

Théorème. Si τ appartient à $\mathcal{H} \cap K$, alors $\Phi(\tau)$ appartient à $E(K^{\text{ab}})$.

$K^{\text{ab}} =$ extension abélienne maximale de K.

Version plus précise: Si $\tau \in \mathcal{H}$ est un nombre quadratique, soit

$$F_\tau(x, y) = Ax^2 + Bxy + Cy^2$$

la forme quadratique binaire primitive telle que

$$F_\tau(\tau, 1) = 0, \quad N|A.$$

On pose $\text{Disc}(\tau) := \text{Disc}(F_\tau)$, et

$$\mathcal{H}^D := \{\tau \text{ t.q. } \text{Disc}(\tau) = D.\}.$$

Théorie du corps de classe

$$G_D := \left\{ \begin{array}{c} \text{Classes de formes quadratiques} \\ \text{binaires de discriminant } D \end{array} \right\}.$$

Cet ensemble est un *groupe abélien* pour la loi de composition de Gauss.

La théorie du corps de classe

$$\text{rec} : G_D \longrightarrow \text{Gal}(H_D/K),$$

où

H_D = corps de classe d'anneau (“ring class field”) de K associé à D.

Points de Heegner

Théorème Si τ appartient à $\mathcal{H}^D$, alors $\Phi(\tau)$ appartient à $E(H_D)$, et les applications sont compatibles aux actions dans le diagramme suivant:

$$\begin{array}{ccc} G_D & \stackrel{\text{rec}}{\longrightarrow} & \mathrm{Gal}(H_D/K) \\ \circlearrowleft & & \circlearrowleft \\ \mathcal{H}^D/\Gamma_0(N) & \stackrel{\Phi}{\longrightarrow} & E(H_D) \end{array}$$

Interets de cette construction

$\boxed{\text{1. Construction de points de } E(\mathbf{Q})}$

$$P_D := \mathrm{Trace}_{H_D/\mathbf{Q}}(\Phi(\tau)), \quad \tau \in \mathcal{H}^D.$$

Théorème (Kolyvagin) Si $r := \mathrm{rang}(E(\mathbf{Q})) \neq 1$, alors P_D est un point de torsion.

Théorème (Gross-Zagier). Supposons que la conjecture de Birch et Swinnerton-Dyer est vraie. Si $r = 1$, alors P_D est un point d'ordre infini.

$\boxed{\text{2. Construction d'extensions abéliennes}}$

$\mathbf{Q}^{\mathrm{ab}} = \cup_{\alpha\in\mathbf{Q}} \mathbf{Q}(e^{2\pi i\alpha})$,

$K^{\mathrm{ab}} \simeq \cup_{\substack{\alpha\in\mathbf{Q} \\ \tau\in\mathcal{H}\cap K}} K(e^{2\pi i\alpha}, j(\tau))$,

où j= la fonction modulaire j sur $\mathcal{H}/\mathbf{SL}_2(\mathbf{Z})$.

Question Naturelle: Qu'arrive-t-il si K est un corps quadratique *réel*?

Corps quadratiques réels

On ne dispose pas de "théorie explicite du corps de classe" pour les corps quadratiques réels.

On aimerait étendre, de facon au moins *conjecturale*, la théorie de la multiplication complexe, et la construction des points de Heegner, aux corps quadratiques réels.

Ingrédients:

1. Analyse p-adique.

2. Variation p-adique des formes modulaires ("Théorie de Hida").

Analyse p-adique

On suppose que E est de conducteur $N = pM$, avec $p \nmid M$.

$\mathbf{Q}_p :=$ complétion de $\mathbf{Q}$ pour la valuation p-adique.

$\mathbf{C}_p :=$ complétion de $\bar{\mathbf{Q}}_p$.

$\mathcal{H}_p := \mathbf{C}_p - \mathbf{Q}_p$. (Un analogue p-adique de $\mathcal{H}$)

On fixe K un corps quadratique réel, muni de plongements dans $\mathbf{R}$ et dans $\mathbf{C}_p$.

Motivation (naive): $\mathcal{H} \cap K = \emptyset$, mais $\mathcal{H}_p \cap K$ peut être non-vide!

But: Définir une "paramétrisation modulaire" p-adique

$$\Phi : \mathcal{H}_p^D / \Gamma_0(N) \longrightarrow E(H_D),$$

pour des discriminants D *positifs*.

Théorie de Hida

Soit U un disque p-adique $\mathbf{Q}_p$ avec $2 \in U$;

$\mathcal{A}(U) =$ anneau des fonctions p-adiques analytiques sur U.

Théorème. (Hida) Il existe une q-expansion formelle

$$f_\infty = \sum_{n=1}^{\infty} \underline{a}_n q^n, \qquad \underline{a}_n \in \mathcal{A}(U),$$

telle que, pour tout $k \geq 2$, $k \in \mathbf{Z}$, $k \equiv 2 \pmod{p-1}$,

$$f_k := \sum_{n=1}^{\infty} \underline{a}_n(k) q^n$$

est une forme modulaire de poids k sur $\Gamma_0(N)$ (vecteur propre pour les opérateurs de Hecke), et

$$f_2 = f_E.$$

Théorie d'Eichler-Shimura

$\mathcal{P}_k$:= espace des polynômes homogènes de degré $k-2$ à coefficients rationnels.

Théorème. (Shimura) Si f est de poids k, il existe un nombre Ω_f^+ tel que, pour tout $P \in \mathcal{P}_k$, et pour tout $r, s \in \mathbf{P}_1(\mathbf{Q})$,

$$I_f(r,s,P) := (\Omega_f^+)^{-1}\,\mathrm{Re}\left(\int_r^s f(z)P(z,1)dz\right)$$
$$\text{appartient à } \mathbf{Q}(a_1,\ldots,a_n,\ldots).$$

Ces intégrales *déterminent complètement* la forme modulaire f.

Eichler-Shimura pour les familles de Hida

Théorème (Mazur). Pour tout $r, s \in \mathbf{P}_1(\mathbf{Q})$, il existe une mesure p-adique $\mu_{r,s}$ à support compact sur $\mathcal{W} := \mathbf{Q}_p^2 - \{0\}$ tel que, pour tout $P \in \mathcal{P}_k$,

$$\int_{\mathcal{W}} P(x,y) d\mu_{r,s}(x,y) = \lambda_k I_{f_k}(r,s,P)$$

$$=: \tilde{I}_{f_k}(r,s,P),$$

où λ_k dépend de k, mais pas de r, s, et P.

Les mesures $\mu_{r,s}$ de Mazur permettent de reconstituer les périodes de Shimura attachées aux formes modulaires f_k obtenues par spécialisation de la famille de Hida.

Points de Heegner pour les corps quadratiques réels

Définition. Etant donné $\tau \in \mathcal{H}_p^D/\Gamma_0(M)$, soit $\gamma_\tau \in \Gamma_0(M)$ un générateur de $\mathrm{Stab}_{\Gamma_0(M)}(\tau)$.

Soit log un logarithme p-adique.

On choisit un point base $r \in \mathbf{P}_1(\mathbf{Q})$ quelconque, et on définit une période J_τ par:

$$\begin{aligned} J_\tau &:= \frac{d}{dk}\tilde{I}_{f_k}(r, \gamma_\tau r, (X-\tau Y)^{k-2})|_{k=2} \\ &= \int_{\mathcal{W}} \log(x-\tau y) d\mu_{r,\gamma_\tau r}(x,y). \end{aligned}$$

Le nombre p-adique J_τ ne dépend pas du choix de r.

Points de Heegner pour les corps quadratiques réels

Soit

$$\exp_E : \mathbf{C}_p \longrightarrow E(\mathbf{C}_p)$$

l'exponentielle sur E. Grâce à la période J_τ, on définit:

$$\boxed{\Phi(\tau) := \exp_E(J_\tau)}$$

Conjecture. Si τ appartient à $\mathcal{H}_p^D$, alors $\Phi(\tau)$ appartient à $E(H_D)$, et les applications sonts compatibles aux actions dans le diagramme suivant:

$$\begin{array}{ccc} G_D & \xrightarrow{\text{rec}} & \mathrm{Gal}(H_D/K) \\ \circlearrowleft & & \circlearrowleft \\ \mathcal{H}_p^D/\Gamma_0(M) & \xrightarrow{\Phi} & E(H_D). \end{array}$$

Un exemple

Conducteur $N = 11$.

$$E : y^2 + y = x^3 - x^2 - 10x - 20$$

La conjecture sur les “points de Stark-Heegner” a pu être utilisée pour calculer efficacement des points sur E à coordonnées dans les extensions abéliennes de corps réels quadratiques, au moyen de l’analyse 11-adique, grâce à un ensemble de programmes en `Magma` appelé `shp`. (Travail en collaboration avec Robert Pollack.)

Insérer ici la page de mon article avec Pollack.

Un autre exemple

L'équation

$$\boxed{y^2 - y = x^3 - x}$$

"Quels nombres (rationnels, algébriques) peuvent s'exprimer à la fois comme un produit de deux et de trois nombres consécutifs?"

$N = 37$; ce problème, sur les corps de classe des corps quadratiqes réels, se prête donc à une attaque par de l'anayse 37-adique!

$D > 0$, $h =$ nombre de classes de D.

$$P_1 = (x_1, y_1), \ldots, P_h = (x_h, y_h)$$

$$h_D(x) = \prod_{j=1}^{h} (x - x_j).$$

Insérer ici la page de mon article avec Pollack.