Exemples et calculs de points de Heegner

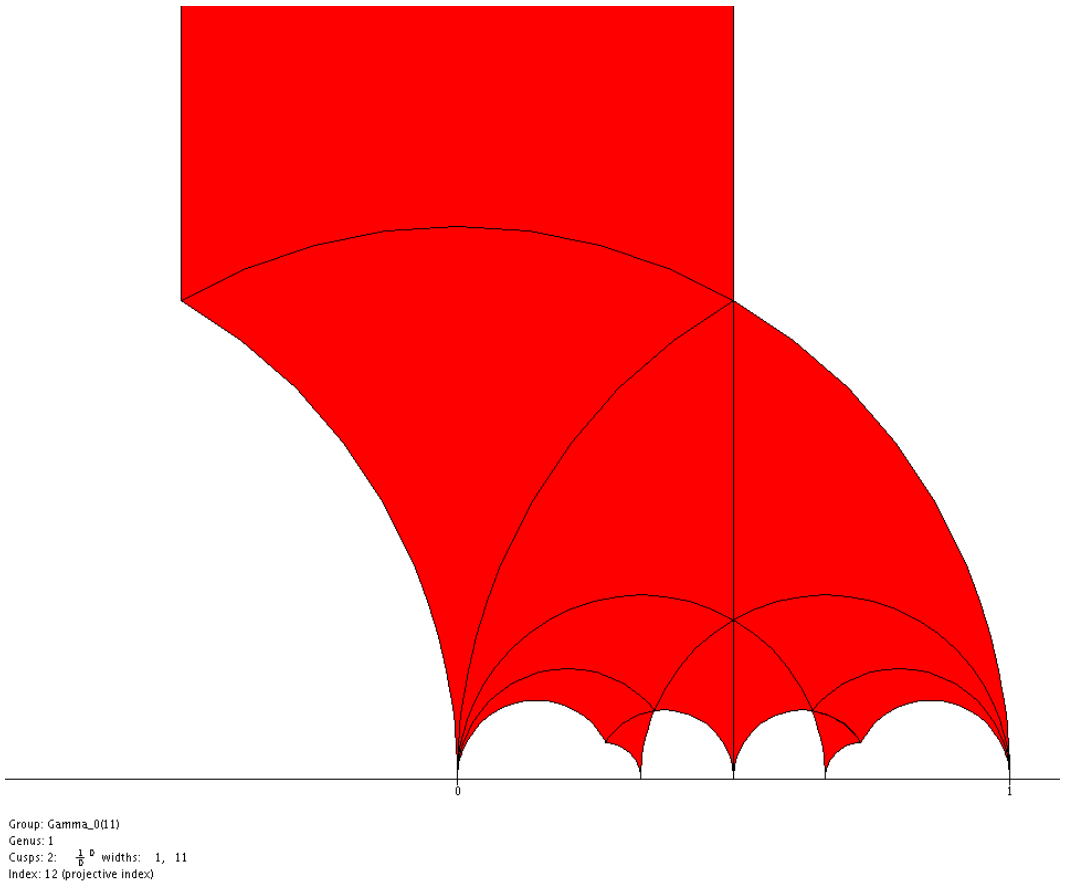
christian wuthrich

27 mars 07

La paramétrisation modulaire de $X_0(11)$

Partons du groupe

$$\Gamma = \Gamma_0(11) = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \,|\, c \equiv 0 \pmod{11} \}\,.$$



La paramétrisation modulaire de $X_0(11)$

Partons du groupe

$$\Gamma = \Gamma_0(11) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \,|\, c \equiv 0 \pmod{11}\}\,.$$

On trouve une base de l'espace $M_2(\Gamma_0(11))$ des formes modulaires de poids 2 pour Γ avec $q = e^{2\pi i \tau}$.

```
sage : M2 = ModularForms(Gamma0(11)); B = M2.basis(); show(B)
```

$$[q - 2q^2 - q^3 + 2q^4 + q^5 + O(q^6),$$
$$1 + \frac{12}{5}q + \frac{36}{5}q^2 + \frac{48}{5}q^3 + \frac{84}{5}q^4 + \frac{72}{5}q^5 + O(q^6)]$$

En fait, ces deux formes modulaires sont bien connues. La première est

$$f = q \cdot \prod_{n \geqslant 1} (1-q^n)^2 \cdot (1-q^{11n})^2$$

et la seconde est une série d'Eisenstein G. On peut remplacer la deuxième forme par

$$\vartheta^2 = \frac{8}{5} \cdot f + G\,.$$

```
sage : f = B[0].q_expansion(7); G = 5*B[1].q_expansion(7);
th=(G+8*f)/5; show(th)
```

$$1 + 4q + 4q^2 + 8q^3 + 20q^4 + 16q^5 + 32q^6 + O(q^7)$$

ϑ est une série de thêta pour la forme quadratique

$$Q(x,y) = x^2 + x\,y + 3\,y^2$$

de discriminant -11.

$$\vartheta(q) = \sum_{(x,y)\in\mathbb{Z}^2} q^{Q(x,y)}$$

```
sage : %magma Q := QuadraticForms(-11) ! <1,1,3>; R<q> :=
PowerSeriesRing(Integers()); ThetaSeries(Q,11)
```

$$1 + 2q + 4q^3 + 2q^4 + 4q^5 + 6q^9 + O(q^{11})$$

On cherche des fonctions sur $X_0(11)$. Le quotient

$$u = \frac{\vartheta^2}{f}$$

est une fonction sur $X_0(11)$ avec un pôle simple en ∞.

```
sage : u = th/f; show(u)
```

$$\frac{1}{q} + 6 + 17q + 46q^2 + 116q^3 + 252q^4 + 533q^5 + O(q^6)$$

Pour avoir une deuxième fonction sur $X_0(11)$ on pose

$$v = \frac{q \cdot \frac{du}{dq}}{f}.$$

```
sage : v = (u.derivative()*q)/f; show(v)
```

$$\frac{-1}{q^2} + \frac{-2}{q} + 12 + 116q + 597q^2 + 2298q^3 + 7616q^4 + O(q^5)$$

Ça serait trop facile si on avait déjà les bonnes fonctions. Il faut prendre

$$x = \tfrac{1}{2}(u^2 - v - 10\,u + 10)$$
$$y = \tfrac{1}{2}(u^3 - u \cdot v - 15\,u^2 + 5\,v + 28\,u - 12)$$

```
sage : x=(u^2-v-10*u+10)/2;show(x);y=(u^3-u*v-15*u^2+5*v+28*u-12)/2;show(y);
```

$$\frac{1}{q^2} + \frac{2}{q} + 4 + 5q + 8q^2 + q^3 + 7q^4 + O(q^5)$$
$$\frac{1}{q^3} + \frac{3}{q^2} + \frac{7}{q} + 12 + 17q + 26q^2 + 19q^3 + O(q^4)$$

$$x = \frac{1}{q^2} + \frac{2}{q} + 4 + \cdots \qquad y = \frac{1}{q^3} + \frac{3}{q^2} + \frac{7}{q} + 12 + \cdots$$

... on trouve à la fin une expression polynomiale

$$y^2 + y - (x^3 - x^2 - 10\,x - 20)$$

qui donne une fonction holomorphe en $\infty \in X_0(11)$ dont le développement en q est nul.

```
sage : show(y^2 + y - (x^3-x^2-10*x-20))
```

$$0 + \cdots$$

- L'expression (x, y) définit une application

$$\varphi : X_0(11) \to \mathbb{P}^2$$

dont l'image est contenue dans la courbe décrite par cette équation.

- C'est un morphisme surjectif sur une courbe elliptique E, appelée 11a1 :

```
sage : e = EllipticCurve([0,-1,1,-10,-20]); show(e); show(e.label())
```

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

'11a1'

Un point de Heegner

On va construire le point de Heegner sur cette courbe E associé au corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-2})$.

- L'anneau des entiers est $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$.
- Le groupe des classes est trivial.

```
sage : K.<s> = NumberField(x^2+2); show(K); K.class_group()
```

$$\mathbf{Q}[s]/(s^2+2)$$

```
Trivial Abelian Group
```

Pour pouvoir construire un tel point il faut que l'idéal $(11)\mathbb{Z}[\sqrt{-2}]$ se factorise en deux idéaux premiers.

$$(11) = \mathfrak{p} \cdot \bar{\mathfrak{p}}$$

En effet :

```
sage : p1,p2 = K.factor_integer(11); p1 = p1[0];p2 = p2[0];show(p1,'*',p2)
```

$$(11, s - 3) * (11, s + 3)$$

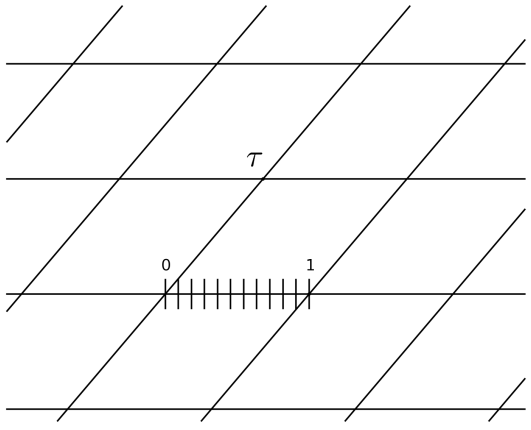
Cet idéal $\mathfrak{p}$ est bien sûr principal et on trouve un générateur $a = 3 - \sqrt{-2}$.

```
sage : a = p1.gens_reduced()[0]; show(a)
```

$$-s + 3$$

- On se rappelle que la courbe $X_0(11)$ paramétrise des couples (A, C) où A est une courbe elliptique et C est un sous-groupe cyclique d'ordre $N = 11$ dans A.
- La correspondance avec la description $\Gamma_0(11) \setminus \mathcal{H}$ se fait par

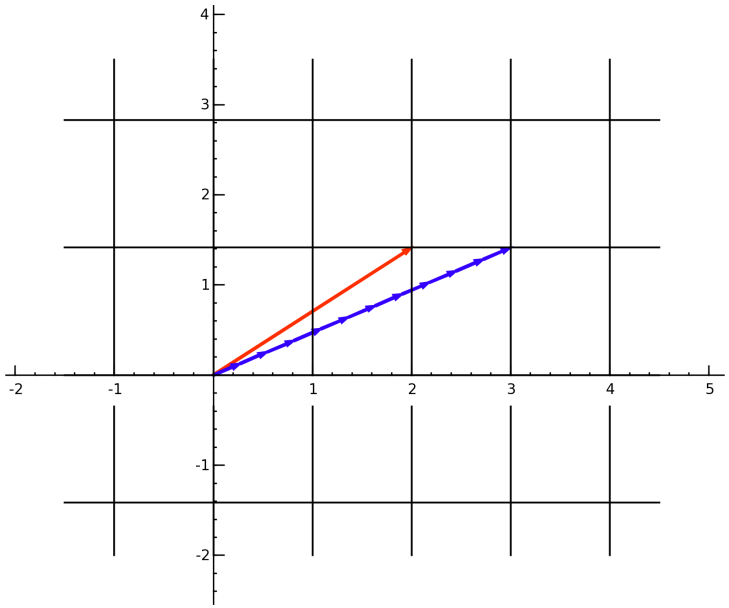
$$\tau \quad \leftrightarrow \quad \left(\mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}, \langle \frac{1}{11} \rangle \right) .$$



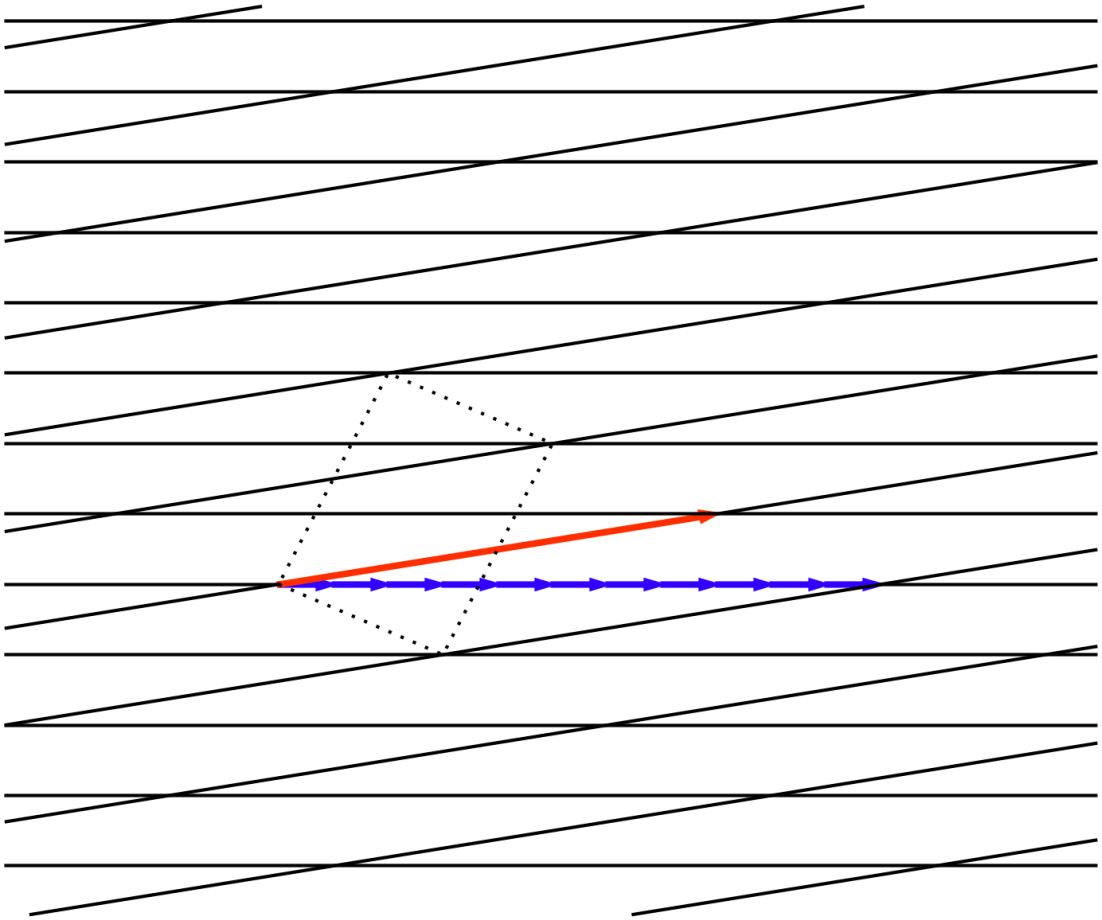
- L'anneau $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$ est un réseau dans $\mathbb{C}$. On a donc une courbe elliptique $A = \mathbb{C}/\mathcal{O}_K$ définie sur $\mathbb{C}$.
- Un sous-groupe de A d'ordre 11 se représente par un réseau dans $\mathbb{C}$ contenant $\mathcal{O}_K$ avec indice 11.
- On peut prendre $\mathfrak{p}^{-1} = a^{-1} \cdot \mathcal{O}_K$ avec

$$\frac{1}{a} = \frac{\bar{a}}{11} = \frac{3+\sqrt{-2}}{11}.$$

- On aimerait représenter le couple $(A, C) = (\mathbb{C}/\mathcal{O}_K, \mathfrak{p}^{-1}/\mathcal{O}_K)$ sous une forme telle que le sous-groupe soit engendré par $\frac{1}{11}$.



- Le premier vecteur ω_1 de la nouvelle base est $3 + \sqrt{-2}$.
- On peut compléter la base avec $\omega_2 = 2 + \sqrt{-2}$ car $\det\left(\begin{smallmatrix} 3 & 1 \\ 2 & 1 \end{smallmatrix}\right) = 1$.



Ce qui nous donne pour

$$\tau = \frac{\omega_2}{\omega_1}$$

la valeur suivante.

```
sage : omega1 = 3+s; omega2 = s+2;tau = omega2/omega1; show(tau)
```

$$\frac{1}{11}s + \frac{8}{11}$$

C'est donc $\tau = \frac{8+\sqrt{-2}}{11} \in \mathcal{H}$ qui représente la classe modulo $\Gamma_0(11)$ de la courbe $\mathbb{C}/\mathcal{O}_K$ avec le sous-groupe $\mathfrak{p}^{-1}/\mathcal{O}_K$.

Le point de Heegner est $P = \varphi(\tau) = (x(\tau), y(\tau))$. On a $q = e^{2\pi i \tau}$.

```
sage : tau = (8+sqrt(CC(-2)))/11; qh = exp(2*CC(pi)*CC(I)*tau); show(qh)
```

$$-0.063449535689578827100357274632606637751862 52$$
$$-0.441301214019114099088885810862295702100066 \cdot I$$

```
sage : xx = x(qh);show(xx)
```

$$-3.000000000000000000000000000000000000001$$
$$+1.414213562373095048801688724209698078569671 \cdot I$$

```
sage : yy = y(qh);show(yy)
```

$$-3.999999999999999999999999999999999999998$$
$$-4.242640687119285146405066172629094235709017 \cdot I$$

Alors on a trouvé une très bonne approximation de

$$P = (-3 + \sqrt{-2}, -4 - 3\sqrt{-2})\,.$$

```
sage : eK = e.base_extend(K);P = eK([-3 +s,-4-3*s]);show(P)
```

$$(s - 3 : -3s - 4 : 1)$$

C'est un point d'ordre infini dans $E(K)$. On peut montrer que

$$E(K) = {}^{\mathbb{Z}}\!/_{5\mathbb{Z}} \oplus \mathbb{Z} \cdot P\,.$$

Voici la hauteur canonique $\hat{h}(P)$ de P.

```
sage : %magma R<X> :=PolynomialRing(Rationals()); Km<sm> :=NumberField(X^2+2);
E :=EllipticCurve(CremonaDatabase(),11,1,1); EK :=BaseChange(E,Km);
P :=EK![sm-3,-3*sm-4]; print Height(P)
```

$$0.18301909315009310694484484 3$$

Elle est liée à la dérivée de la série L associée à E par la fameuse formule de Gross-Zagier. On trouve que

$$\frac{L'(E/K,1)}{4 \cdot \mathrm{vol}(E)} \sqrt{8} = \hat{h}(P)\,.$$

```
sage : LEK := LSeries(E,Km); lek = magma(Coefficient(LTaylor(LEK,1,2),1));
lek/e.complex_area())/4*sqrt(2)
```

$$0.18301909314990497596939402 5813$$

La conjecture de Birch et Swinnerton-Dyer

$$\frac{L'(E/K,1)}{4 \cdot \mathrm{vol}(E)}\sqrt{8} = \frac{\hat{h}(P) \cdot \#Ш(E/K) \cdot \prod_v c_v}{(\#\mathrm{Torsion}(E(K)))^2}$$

est alors équivalente à

$$\#Ш(E/K) = 1\,.$$

Le théorème de Kolyvagin $(+\,\varepsilon)$ montre ceci et ainsi la conjecture BSD est vérifiée.

La paramétrisation de la courbe 37a1

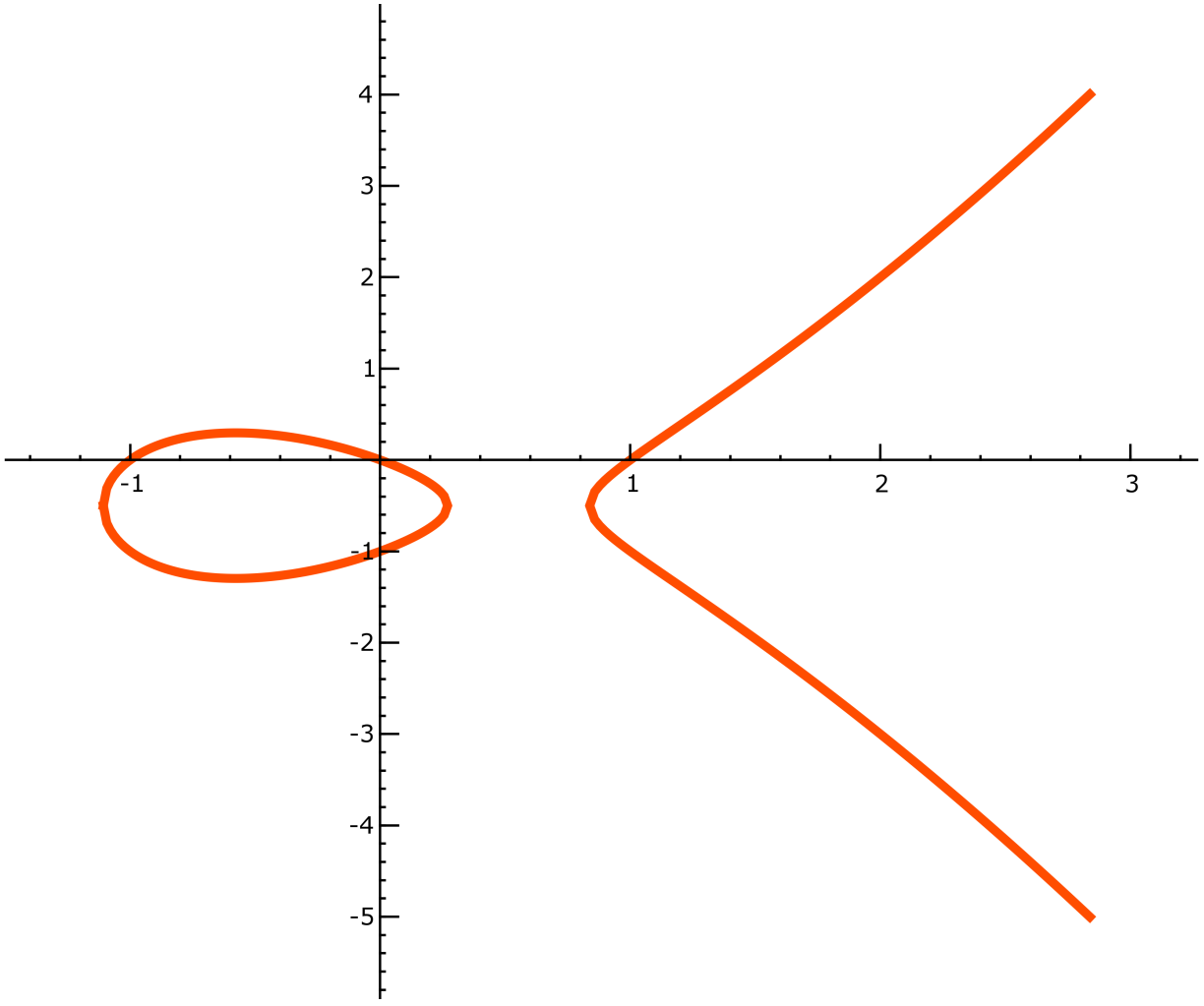
Considérons la courbe 37a1 donnée par l'équation

```
sage : e = EllipticCurve('37a1'); show(e)
```

$$y^2 + y = x^3 - x\,.$$

- Elle possède un point évident $P = (0, 0)$ dans $E(\mathbb{Q})$.
- On montre que $E(\mathbb{Q}) = \mathbb{Z} \cdot P$.
- Elle s'appelle aussi $X_0(37)^+$.

```
sage : show(plot(e,hue=0.05,thickness=3))
```



Pour un premier $p \neq 37$, l'équation $y^2 + y = x^3 - x$ est une courbe elliptique $\tilde{E}$ sur $\mathbb{F}_p$. On pose

$$a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)\,.$$

Par exemple $a_2 = -2$, $a_3 = -3$, $a_{17} = 0$,...

```
sage : e.base_extend(GF(2)).points()
```

$$[(0:1:0), (1:0:1), (0:1:1), (0:0:1), (1:1:1)]$$

Le théorème de Hasse-Weil affirme que $|a_p| < 2\sqrt{p}$.

On peut étendre la définition à tous les entiers de la manière suivante.

- On pose $a_1 = 1$.
- Si $n = p^{k+1}$ est une puissance d'un premier p, on pose récursivement

$$a_{p^{k+1}} = a_p \cdot a_{p^k} - p \cdot a_{p^{k-1}} \qquad \text{pour tout } k \geqslant 1.$$

- On impose que $a_{nm} = a_n \cdot a_m$ si n et m sont premiers entre eux.

Maintenant on fabrique avec ces nombres une série caractéristique

$$f_E = q + a_2\, q^2 + a_3\, q^3 + a_4\, q^4 + \cdots \quad \in \mathbb{Z}[\![q]\!]\,.$$

```
sage : fe = sum([ e.an(n)*q^n for n in range(1,20)]) + O(q^20) ; show(fe)
```

$$q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + 4q^{10}$$
$$-5q^{11} - 6q^{12} - 2q^{13} + 2q^{14} + 6q^{15} - 4q^{16} - 12q^{18} + O(q^{20})$$

Le théorème de la modularité des courbes elliptiques montre que f_E est une forme modulaire de poids 2 pour $\Gamma_0(37)$.

On peut décrire la paramétrisation modulaire de la manière suivante. Voici la forme différentielle invariante par la loi de groupe sur E.

$$\omega = \frac{dx}{2y+1}$$

Utilisant la paramétrisation modulaire

$$\varphi : X_0(37) \to E$$

on obtient

$$\varphi^*(\omega) = f_E(q) \cdot \frac{dq}{q} = 2\pi i \cdot f_E(\tau)\, d\tau\,.$$

On décompose φ.

$$\begin{array}{ccccc} X_0(37) & \xrightarrow{\phi} & \mathbb{C}/\Lambda_E & \longrightarrow & E \\ f_E \dfrac{dq}{q} & \longmapsto & dz & \longmapsto & \omega \end{array}$$

La première application est donnée par

$$\phi(q) = \int_0^{\phi(q)} dz = \int_0^q f_E \frac{dq}{q} = \sum_{n \geqslant 1} \frac{a_n}{n} q^n$$

et la deuxième s'obtient à partir de la fonction de Weierstrass $\wp(z)$ associée à E.

On peut calculer les points de Heegner sur 37a1 associés au corps $\mathbb{Q}(\sqrt{-83})$.
On trouve comme avant la classe modulo $\Gamma_0(37)$

$$\tau = \frac{19 + \sqrt{-83}}{74}.$$

```
sage : tau = (sqrt(CC(-83)) + 19 )/ 74;qh= exp(2*CC(I)*CC(pi)*tau);show(qh)
```

$$-0.019581236641462602257258671738562186415457$$
$$+0.460957555681879973113840982514950867245073 9 * I$$

```
sage : z = sum([e.an(n)/n*qh^n for n in range(1,6000)]);show(z)
```

$$0.194140444318338009176536401944075106218875 5$$
$$+0.570819148183218962908580932610019188566460 1 * I$$

En utilisant la fonction de Weierstrass on trouve le point de Heegner.

```
sage : ep = pari(e);P = ep.ellztopoint(z);show(P)
```

$$[-2.23898362150450623732346254067108755072377$$
$$-1.62766911780350485424881450840976354738452 03 * I,$$
$$3.35320996419932442948310133257738845727070 56$$
$$-2.40564163857095761182902421605374854012393 03 * I]$$

Ce n'est pas un point sur $K = \mathbb{Q}(\sqrt{-83})$ car $\mathrm{Cl}(K) = \mathbb{Z}/3\mathbb{Z}$.

La coordonnée x de P satisfait au polynôme

```
sage : f=P[0].algdep(3,100); show(f)
```

$$x^3 + 5\,x^2 + 10\,x + 4\,.$$

$H = K[x]/(x^3 + 5x^2 + 10x + 4)$ est le corps de classes de K.

Soit I_1 et I_2 deux idéaux qui représentent les classes non triviales de Cl(K).
On peut calculer les points de Heegner en partant de

$$(A, C) = (\mathbb{C}/I_j, I_j \cdot \mathfrak{p}^{-1}/I_j)\,.$$

La somme des trois points de Heegner, c.-à-d. la trace de P dans K, est

```
sage : ...
```

$$[1.898 \cdot 10^{-119} + 2.262 \cdot 10^{-120} \cdot I,$$
$$-1.898 \cdot 10^{-119} - 2.262 \cdot 10^{-120} \cdot I]\,.$$

Il s'agit du générateur $P = (0, 0)$ de $E(\mathbb{Q})$.

Résumé

Il y a trois situations pour les points de Heegner :

- Si $L(E/\mathbb{Q},1) \neq 0$, alors on peut trouver une extension quadratique imaginaire $K/\mathbb{Q}$ telle qu'il existe un point Heegner d'ordre infini dans $E(K)$. On en déduit la finitude de $E(\mathbb{Q})$ et de $Ш(E/\mathbb{Q})$.
- Si $L(E/\mathbb{Q},1) = 0$ et $L'(E/\mathbb{Q},1) \neq 0$, alors on trouve $K/\mathbb{Q}$ telle que le point de Heegner associé à K donne un point d'ordre infini dans $E(\mathbb{Q})$. On en déduit que le rang de $E(\mathbb{Q})$ est 1 et que $Ш(E/\mathbb{Q})$ est fini.
- Si $L(E/\mathbb{Q},1) = L'(E/\mathbb{Q},1) = 0$ alors les traces de points de Heegner sont de torsion.

Un nombre congruent

Le point de Heegner sur la courbe (pour $D = -31$)

$$y^2 = x^3 - 157^2\, x\,.$$

```
sage : e = EllipticCurve([0,0,0,-157^2,0]);P =
magma(e).HeegnerPoint(nvals=2);show(P[1])
```

$$\left(\frac{-16613623166818526754080 4}{28256306942511458580 25}, \frac{-16766162445683433540481211146978 2006}{15020109520013551810876147023 5125}\right)$$

Ceci nous donne les côtés du triangle d'aire 157.

```
sage : a = (P[1]^2-157^2)/P[2];b = 2*157*P[1]/P[2];c =
(P[1]^2+157^2)/P[2];show((a,b,c))
```

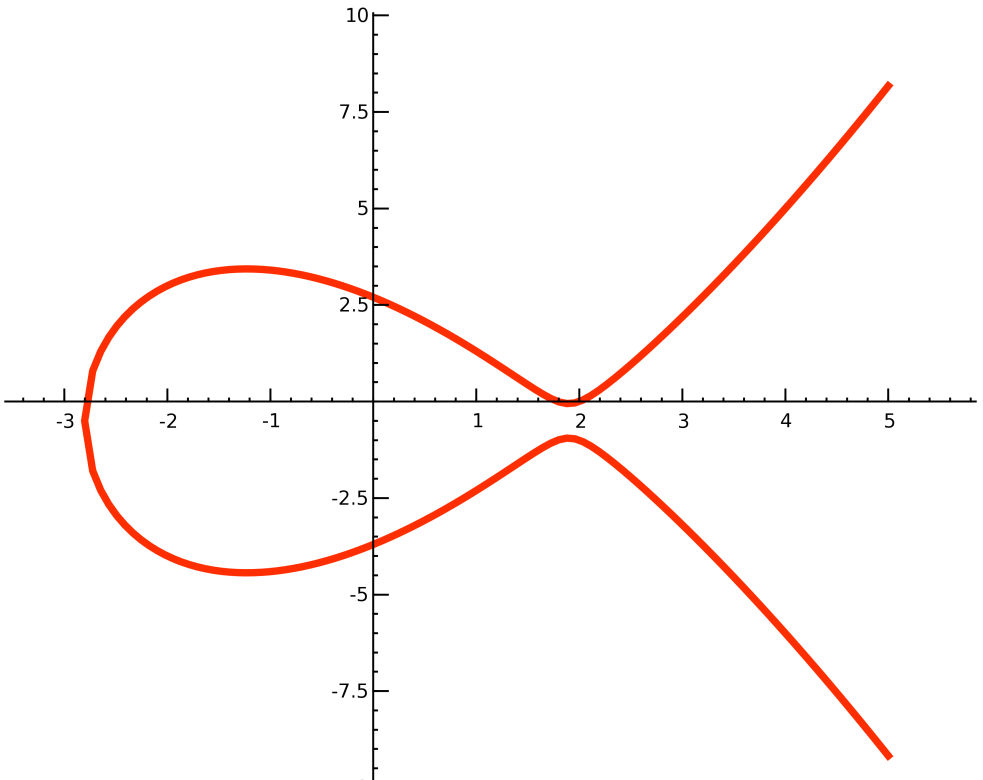
$$\left(\frac{411340519227716149383203}{21666555693714761309610}, \frac{68032984878264350512175 40}{41134051922771614938320 3}, \frac{-22440351770433696992455751309067486316094847 2041}{89123322689288595880255351789671635700164808 30}\right)$$

La courbe 121b1

La courbe 121b1 donnée par

$$y^2 + y = x^3 - x^2 - 7x + 10$$

est à multiplication complexe par $\mathcal{O}_F = \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$.
L'anneau $\mathcal{O}_F$ est principal.



La forme modulaire associée est une série thêta. On a un caractère

$$\varepsilon\colon \mathcal{O}_F \twoheadrightarrow \mathcal{O}_F/(\sqrt{-11}) = \mathbb{F}_{11} \xrightarrow{(\frac{\cdot}{11})} \{0,+1,-1\}\,.$$

Pour tout idéal non nul $I=(z)$, on pose $\psi(I)=\varepsilon(z)\cdot z$ et

$$\theta(q) = \sum_{I\neq 0} \psi(I)\cdot q^{\mathrm{N}(I)}$$

```
sage : th = sum([eps(z)*z*q^(z.norm()) for z in zs])/2;show(th+O(q^20))
```

$$q - q^3 - 2q^4 - 3q^5 - 2q^9 + 2q^{12} + 3q^{15} + 4q^{16} + O(q^{20})$$

Notez que $|a+b\cdot\frac{1+\sqrt{-11}}{2}| = a^2+ab+3b^2 = Q(a,b)$.

- Alors $\theta = f_E$ est la forme modulaire de poids 2 sur $\Gamma_0(121)$ associée à 121b1.
- On trouve un point de Heegner

```
sage : magma(e).HeegnerPoint(nvals=2)
```

$$(4 : -6 : 1)$$

- La courbe 121b1 s'appelle aussi $X_{\text{non déc.}}(11)$.

- Sur 121b1 il existe un sous-groupe C d'ordre 11 défini sur $\mathbb{Q}$.
- Le quotient E/C est la courbe 121b2.

```
sage : e2 = EllipticCurve('121b2');show(e2)
```

$$y^2 + y = x^3 - x^2 - 887x - 10143$$

- Le couple $(121b1, C)$ est alors un élément de $X_0(11)$ défini aur $\mathbb{Q}$.
- On peut calculer son image sur la courbe 11a1 du début utilisant les fonctions x et y.
- On trouve le point $(5, -6)$ d'ordre 5 sur 11a1.