Panorama de la cryptographie des courbes elliptiques

Damien Robert

09/02/2012 (Conseil régional de Lorraine)

La cryptographie, qu'est-ce que c'est ?

Définition

La cryptographie est la science des messages secrets. Elle vise à assurer la confidentialité, l'authenticité et l'intégrité des échanges.

- Une origine ancienne ;
- À l'origine, essentiellement utilisée à des fins militaires ;
- De nos jours, occupe une place primordiale dans notre société de la communication.

Exemple (Chiffrement de César)

MONPREMIERCODESECRET
QSRTVIQMIVGSHIWIGVIX

À l'origine : la cryptographie symmétrique

- Alice et Bob veulent communiquer. Ils se mettent d'accord au préalable sur une clé secrète ;
- Cette clé permet de chiffrer les messages ;
- La même clé permet de les déchiffrer.

Exemple (Chiffrement de Vigenère)

```
LACRYPTOLOGIEPERMETDENVOYERDESMESSAGESCODES
SECRETSECRETSECRETSECRETSECRETSECRETSECRETS
DEEICILSNFKBWTGIQXLHGEZHQITUILEIUJEZWWEFHXK
```

☹ Je veux acheter un pass métrolor de manière sécurisée. Comment faire ?

Le présent : la cryptographie à clé publique

- La solution : utiliser deux clés !
- La clé publique permet de chiffrer les messages. Elle est mise à disposition de tout le monde ;
- La clé secrète permet de déchiffrer les messages. Elle est confidentielle, et on ne peut pas la retrouver à partir de la clé publique !

$\Rightarrow$ Chiffrement asymmétrique ;

$\Rightarrow$ Signatures cryptographiques.

Le futur : le cloud computing

- Stocker les données dans le cloud ⇒ il faut les chiffrer !
- Faire des calculs dans le cloud ? C'est maintenant possible sans avoir à déchiffrer les données au préalable !

Exemple

Données médicales : contrôle d'accès fin sur les données accessibles (à l'assurance, aux médecins...)

Le système RSA

- Pour construire un système à clé publique, il faut une fonction qui soit facile à calculer, dont la réciproque est difficile à calculer ;
- A l'origine, le système RSA : multiplier versus factoriser.

Exemple (Clé RSA 1024 bits)

Clé publique : 135066410865995223349603216278805969938881
475605667027524485143851526510604859533833940287150571
909441798207282164471551373680419703964191743046496589
274256239341020864383202110372958725762358509643110564
073501508187510676594629205563685529475213500852879416
377328 533906109750544334999811150056977236890927563

Cette clé publique est le produit de deux nombres, qui forment la clé secrète.

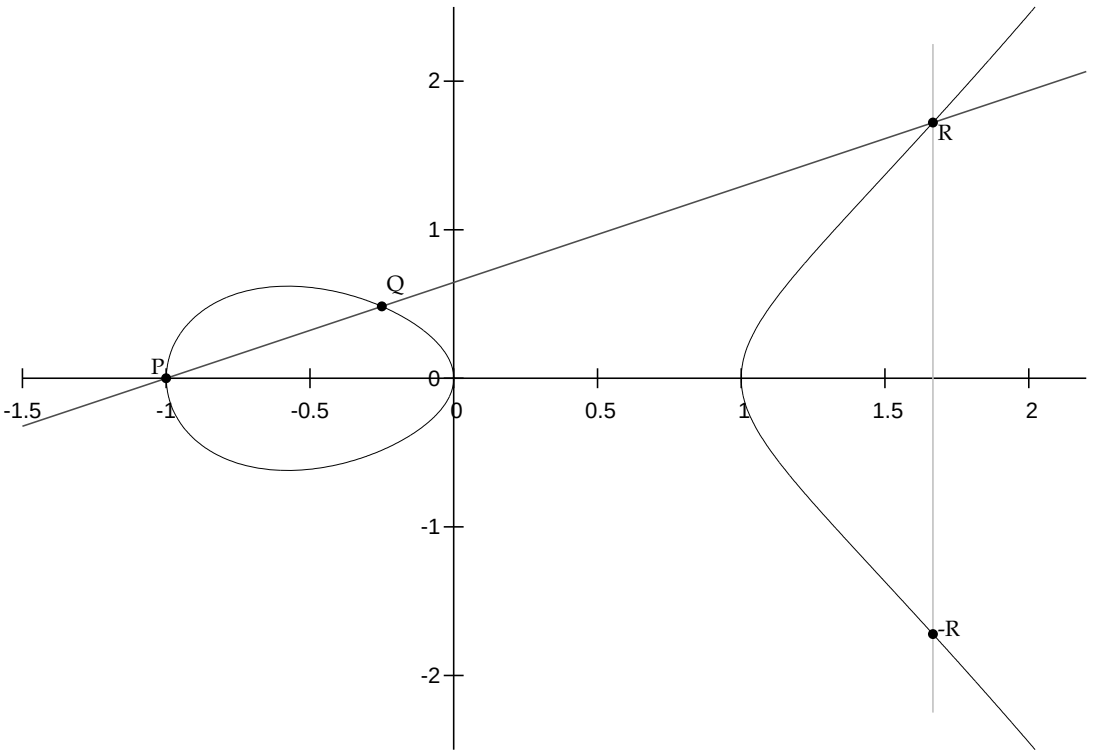
- Système encore majoritaire de nos jours ;
- Utilisé dans les cartes bleues.

Les courbes elliptiques

Définition (car $k \neq 2,3$)

Une courbe elliptique est une courbe plane d'équation

$$y^2 = x^3 + ax + b \qquad 4a^3 + 27b^2 \neq 0.$$



Exponentiation :

$$(\ell, P) \mapsto \ell P$$

Logarithme discret :

$$(P, \ell P) \mapsto \ell$$

Utilisation des courbes elliptiques

Exemple (ECC 160 bits)

- E courbe elliptique $y^2 = x^3 + x + 333$ sur $\mathbb{F}_{1461501637330902918203684832716283019655932542983}$
- Clé publique :

$$P = (136996248758078877499219958849896155834136208629 6,$$
$$407160203592982096299905031630798490942043935021);$$
$$Q = (695697562436343265984113032286189105569389589 80,$$
$$112620361166019022170844963967766792502441296839 5);$$

- Clé secrète : ℓ tel que $Q = \ell P$.

- Utilisées par la NSA ;
- Utilisées dans les passeports biométriques Européens.

Avantage des courbes elliptiques

À niveau de sécurité égale, les cryptosystèmes basés sur les courbes elliptiques, par rapport à RSA sont

- plus rapides ;
- plus compacts ;
- plus puissants.

Exemple (Couplages)

Sur une courbe elliptique, à partir de la clé publique on peut générer d'autres clé publiques. De même pour la clé secrète.
⇒ Certificats anonymes.

Généralisation des courbes elliptiques

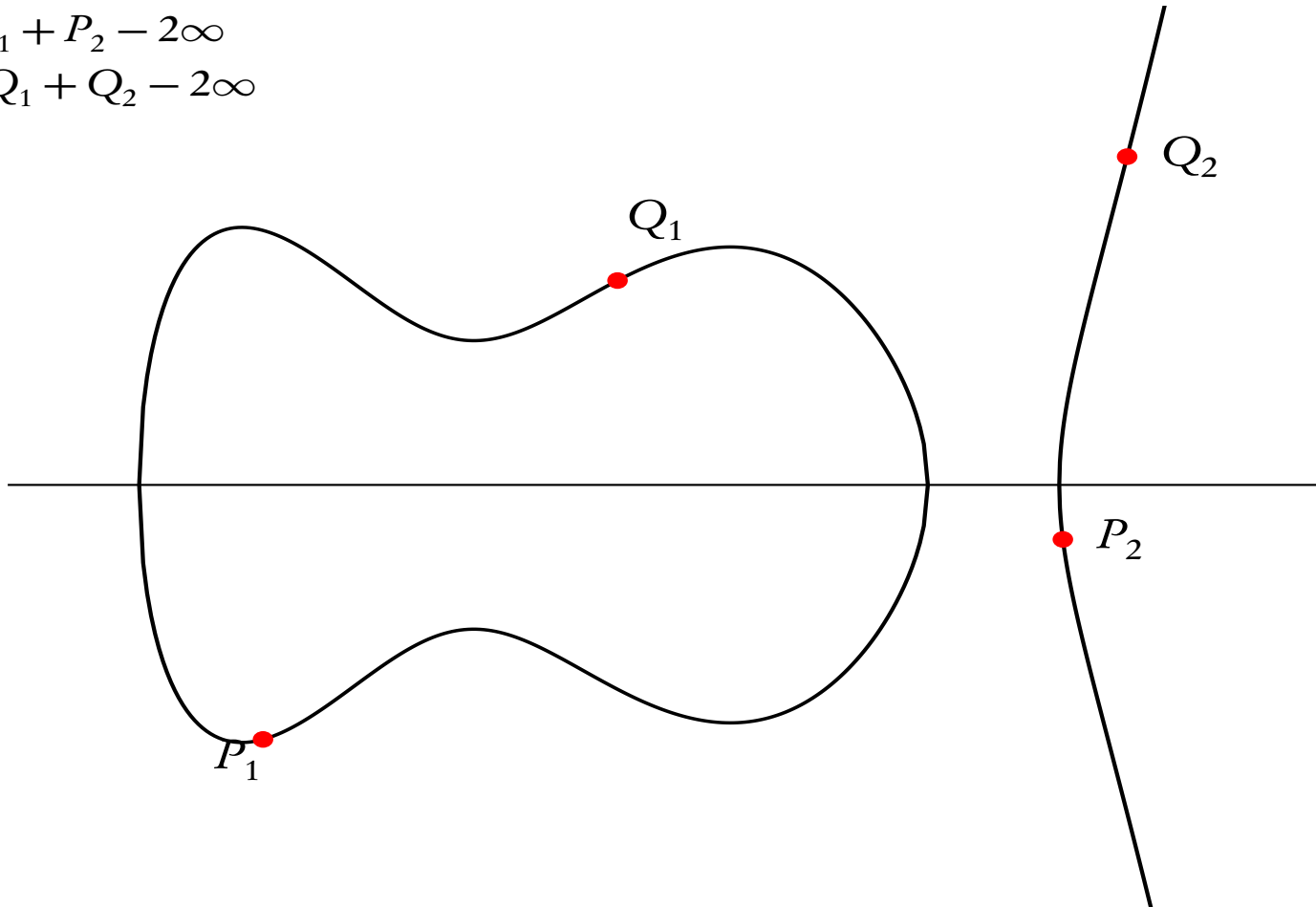
- Garder une génération d'avance : étudier l'équivalent des courbes elliptiques en dimension supérieure (les variétés abéliennes).

Généralisation des courbes elliptiques

Dimension 2 : Loi d'addition sur la Jacobienne d'une courbe hyperelliptique de genre 2 :

$$y^2 = f(x),\ \deg f = 5.$$

$D = P_1 + P_2 - 2\infty$
$D' = Q_1 + Q_2 - 2\infty$

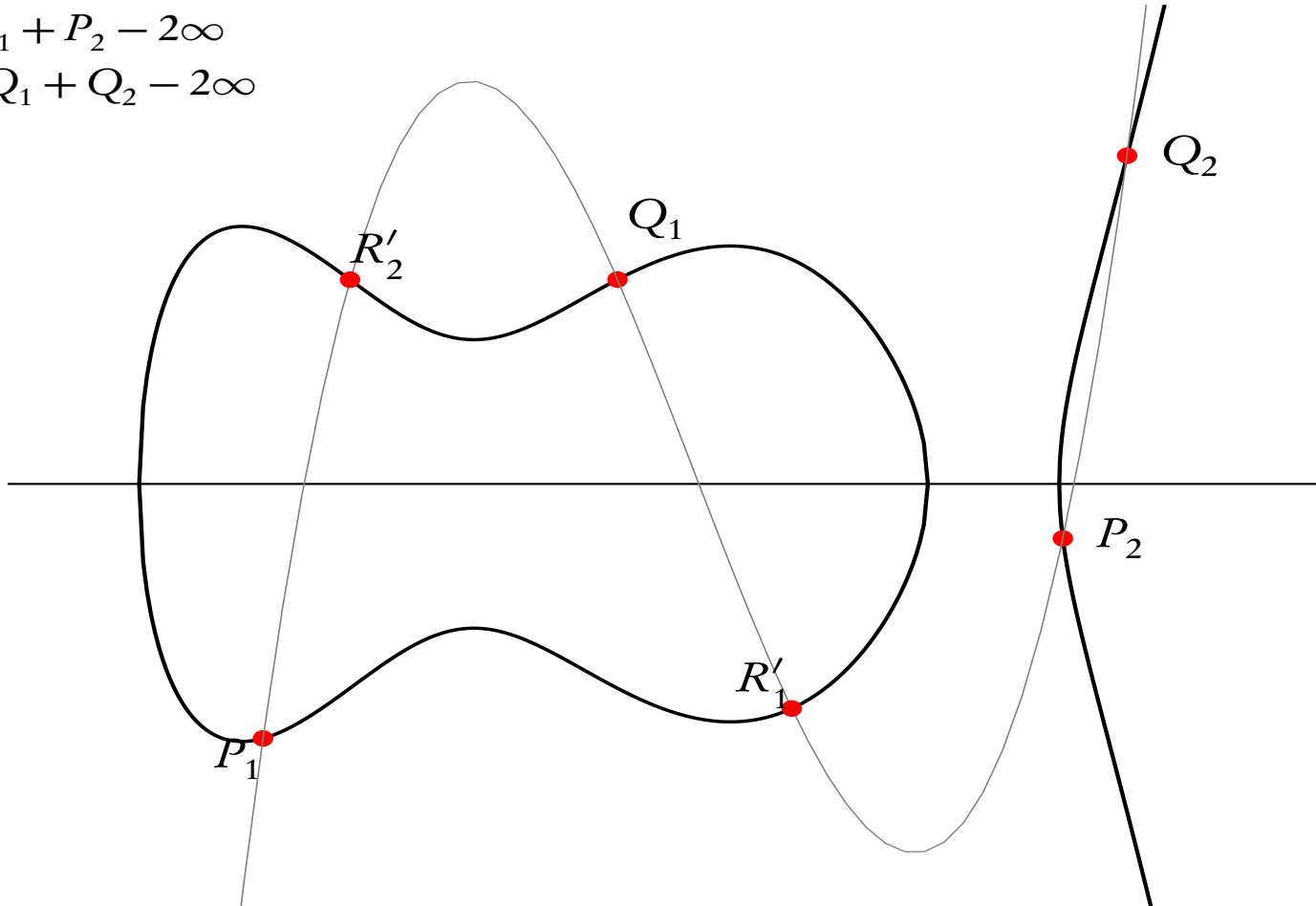


Généralisation des courbes elliptiques

Dimension 2 : Loi d'addition sur la Jacobienne d'une courbe hyperelliptique de genre 2 :

$$y^2 = f(x),\ \deg f = 5.$$

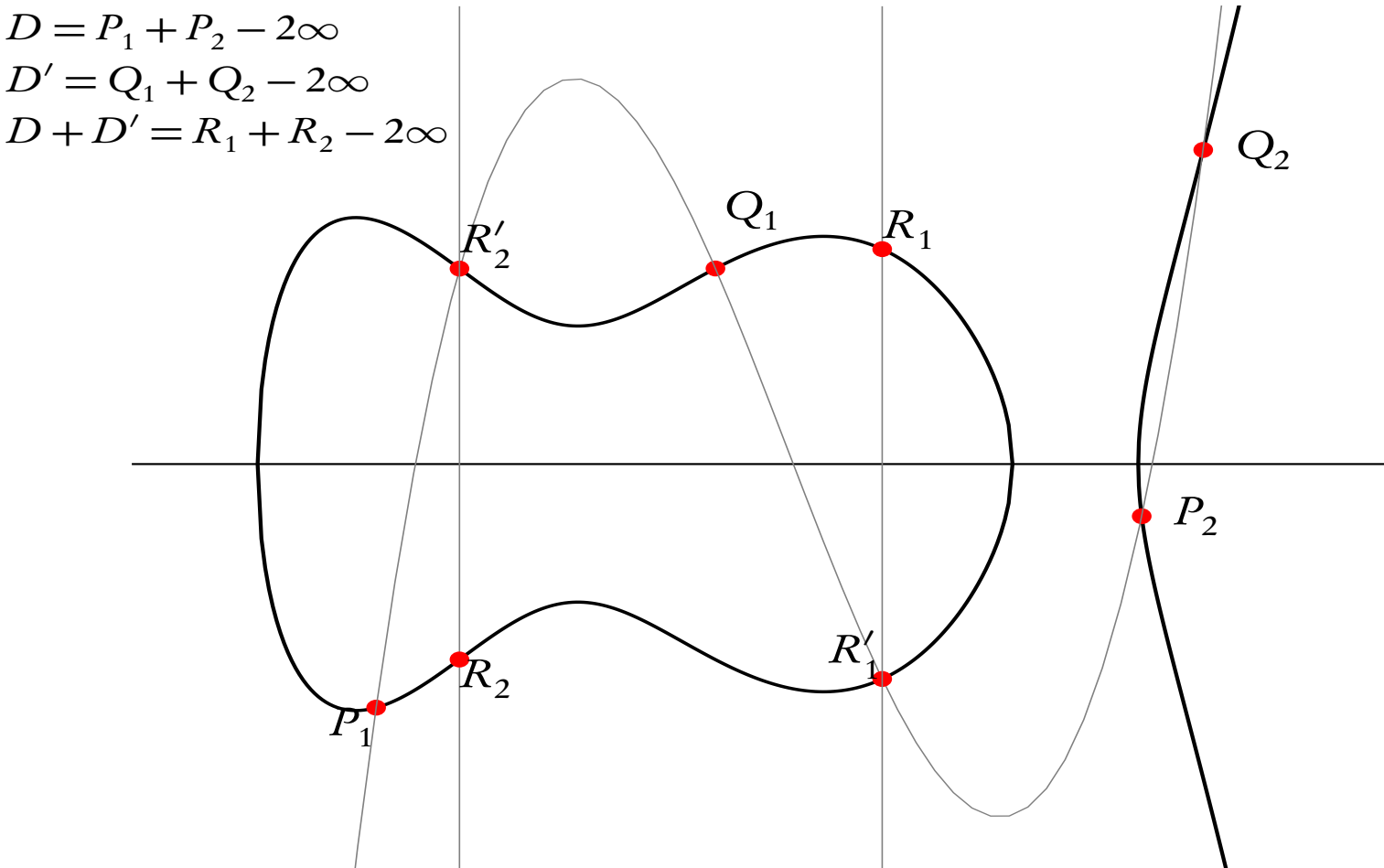
$D = P_1 + P_2 - 2\infty$
$D' = Q_1 + Q_2 - 2\infty$



Généralisation des courbes elliptiques

Dimension 2 : Loi d'addition sur la Jacobienne d'une courbe hyperelliptique de genre 2 :

$$y^2 = f(x),\ \deg f = 5.$$

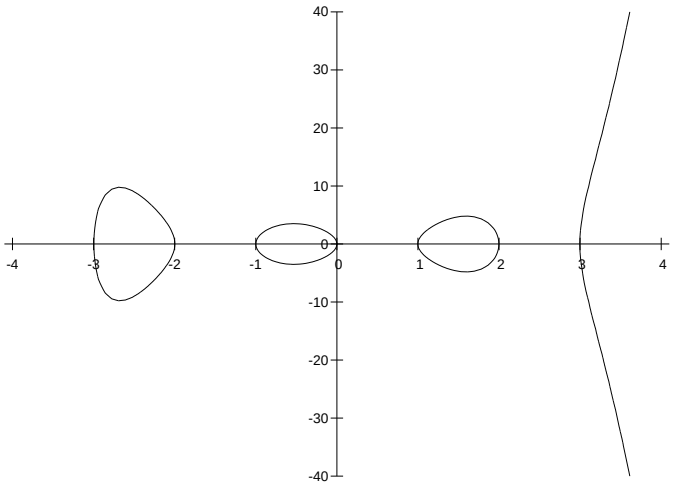


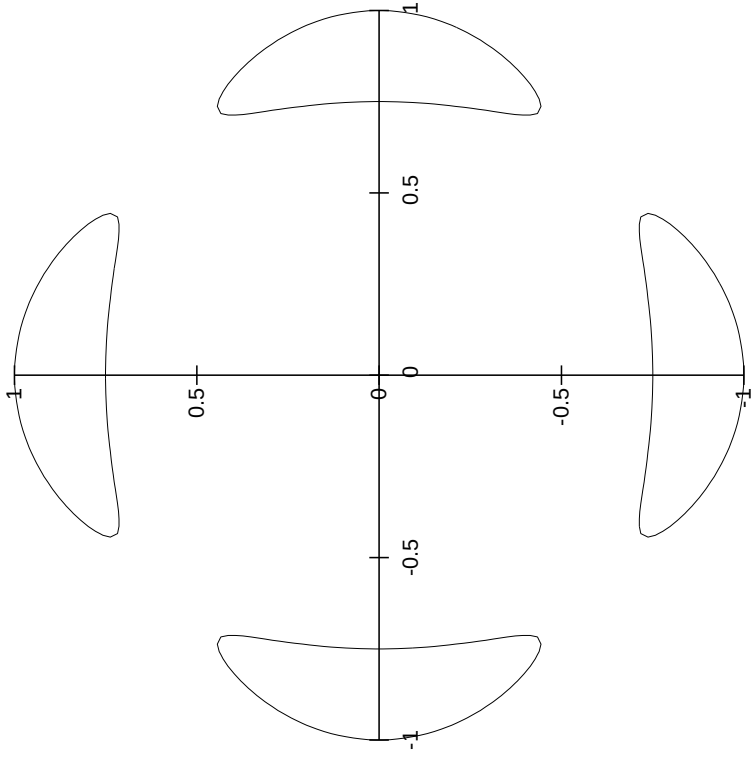
Généralisation des courbes elliptiques

Dimension 3

Jacobiennes de courbes hyperelliptiques de genre 3.

Jacobiennes de quartiques.





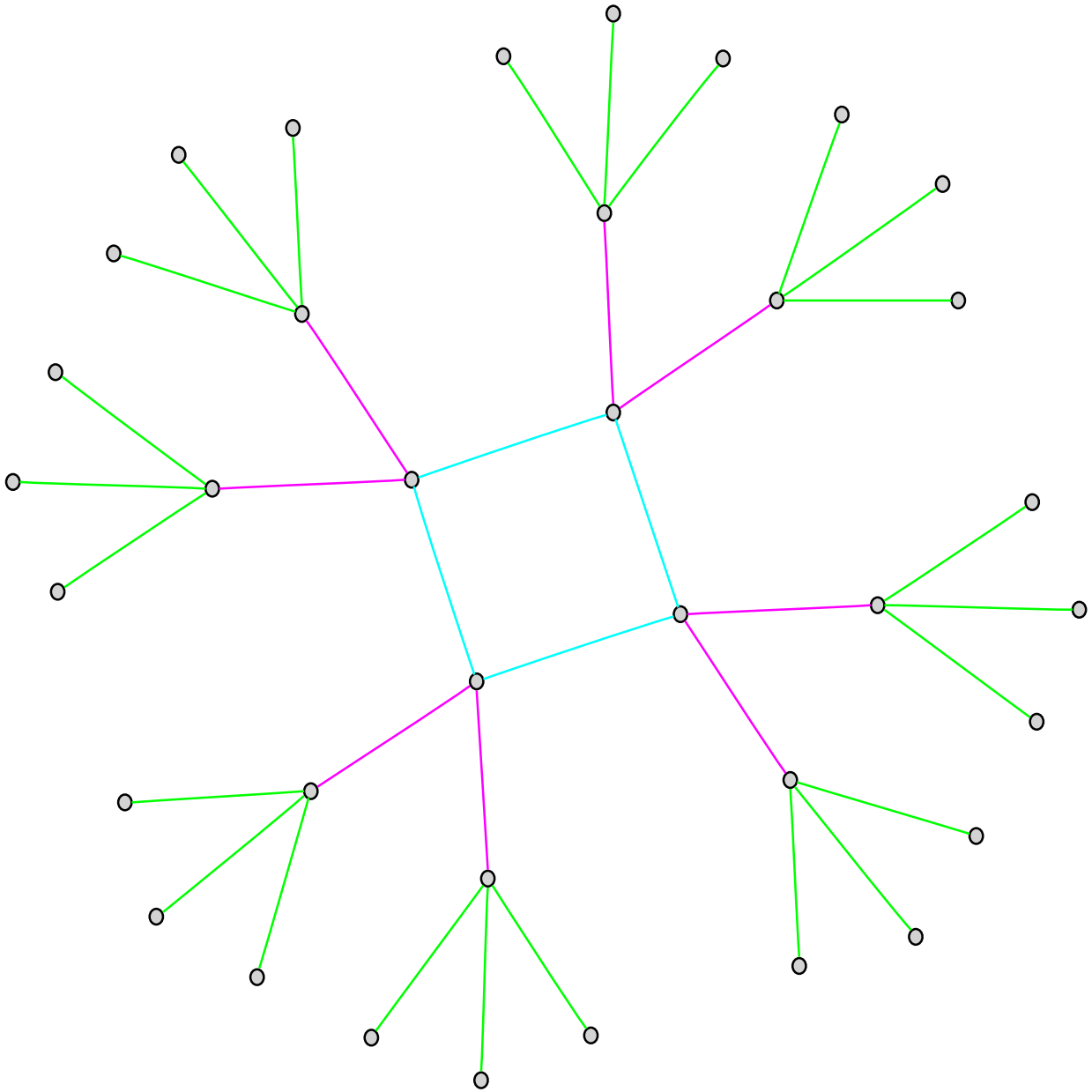
Généralisation des courbes elliptiques

- Garder une génération d'avance : étudier l'équivalent des courbes elliptiques en dimension supérieure (les variétés abéliennes).
- Potentiellement plus efficaces.
- La puissance des courbes elliptiques vient du fait que l'on peut passer d'une courbe à l'autre grâce à des isogénies.

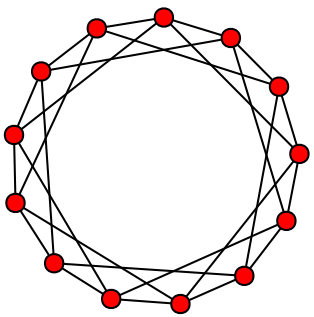
$\Rightarrow$ Calculer des isogénies en dimension supérieure ;

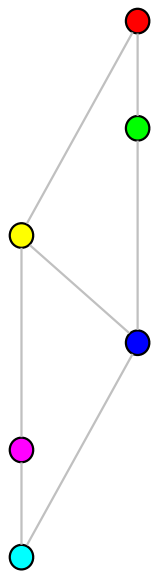
$\Rightarrow$ Comprendre la structures des relations en résultant.

Graphe d'isogénies sur les courbes elliptiques

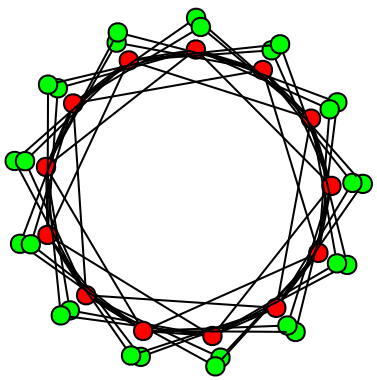


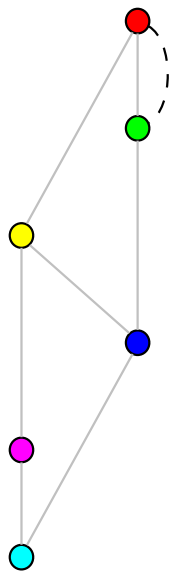
Graphe d'isogénies en dimension 2



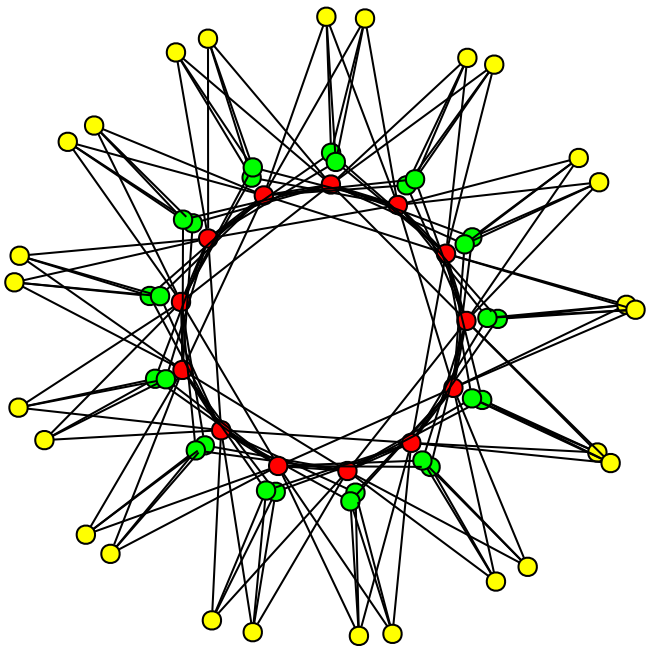


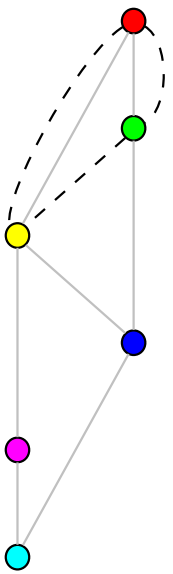
Graphe d'isogénies en dimension 2



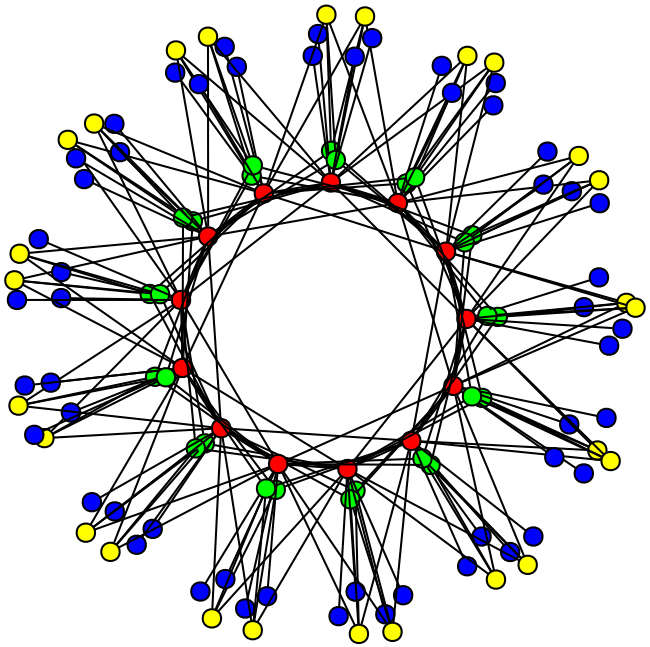


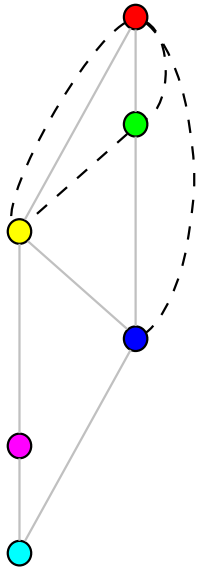
Graphe d'isogénies en dimension 2



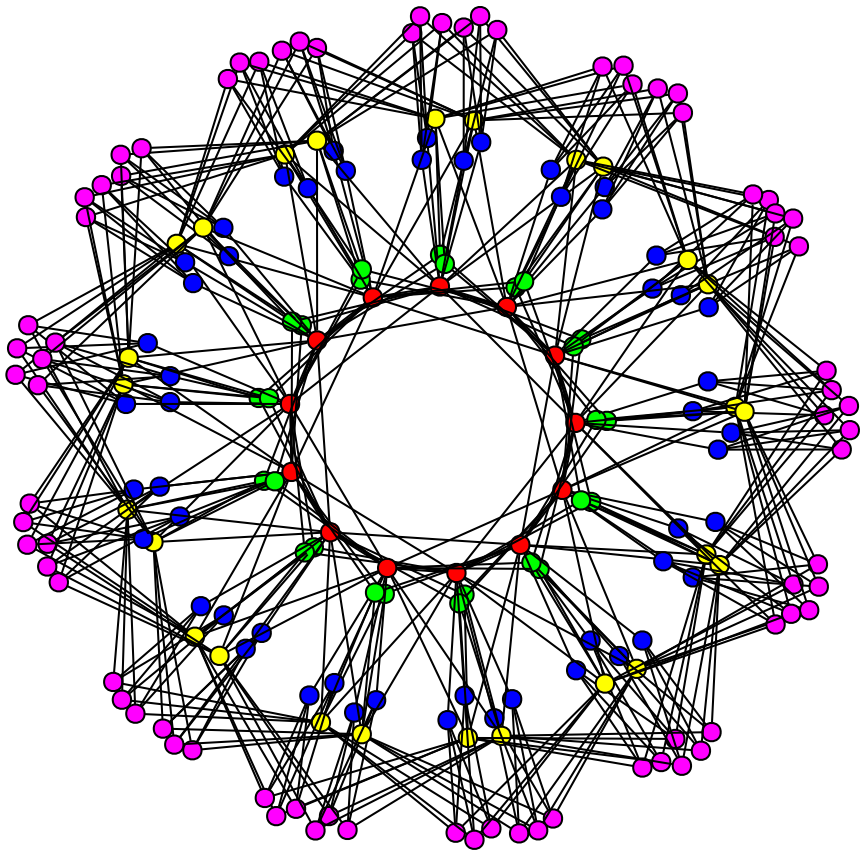


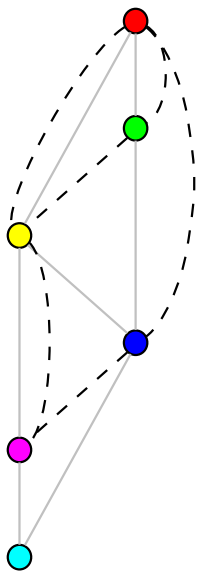
Graphe d'isogénies en dimension 2



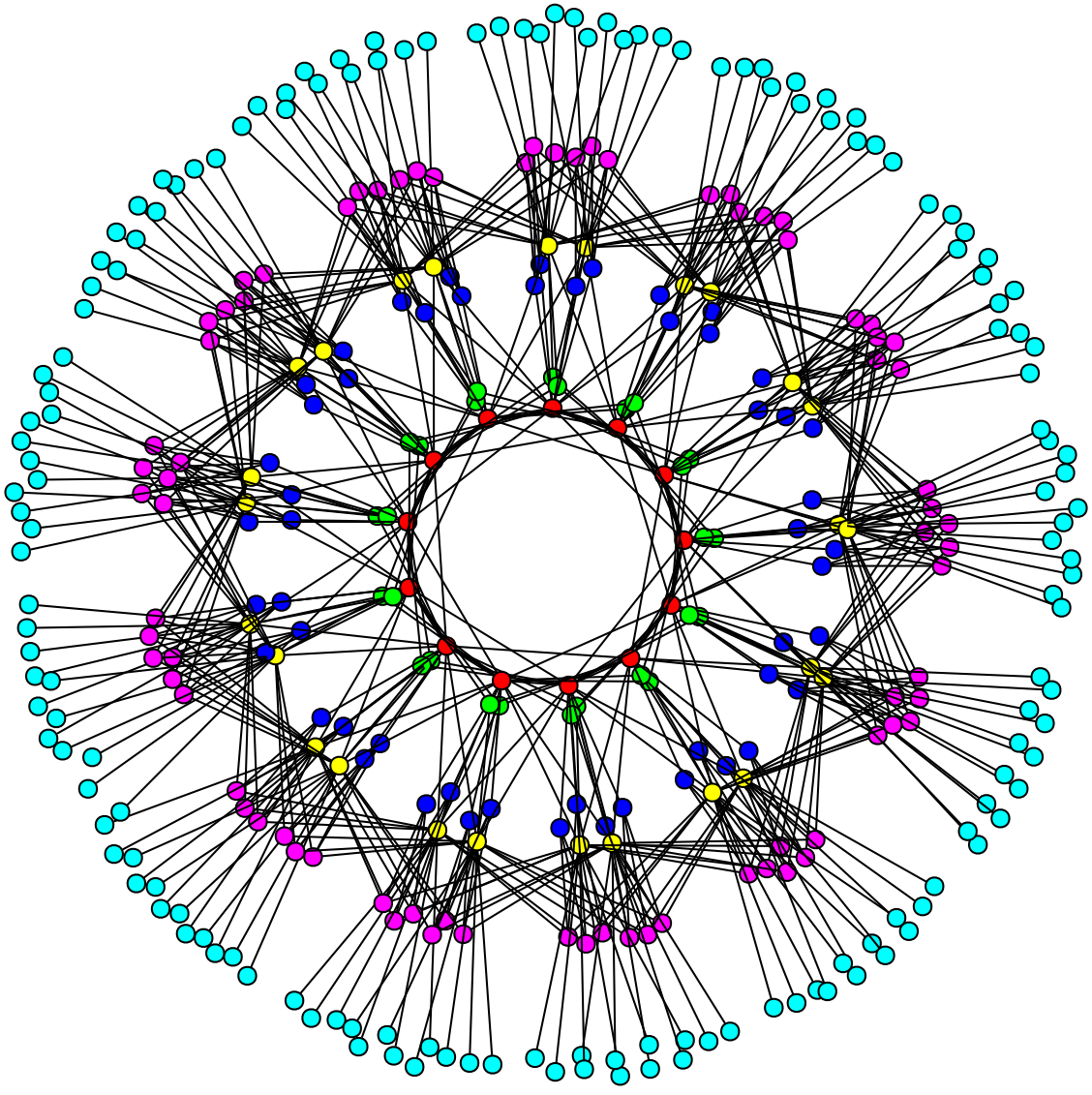


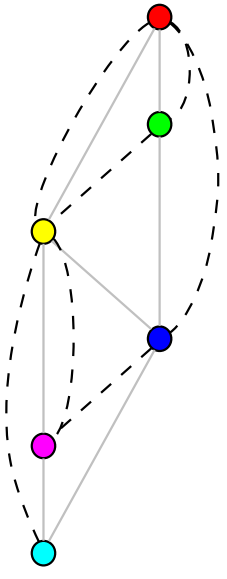
Graphe d'isogénies en dimension 2





Graphe d'isogénies en dimension 2





Merci !