Courbes Elliptiques

Alexandre Duc

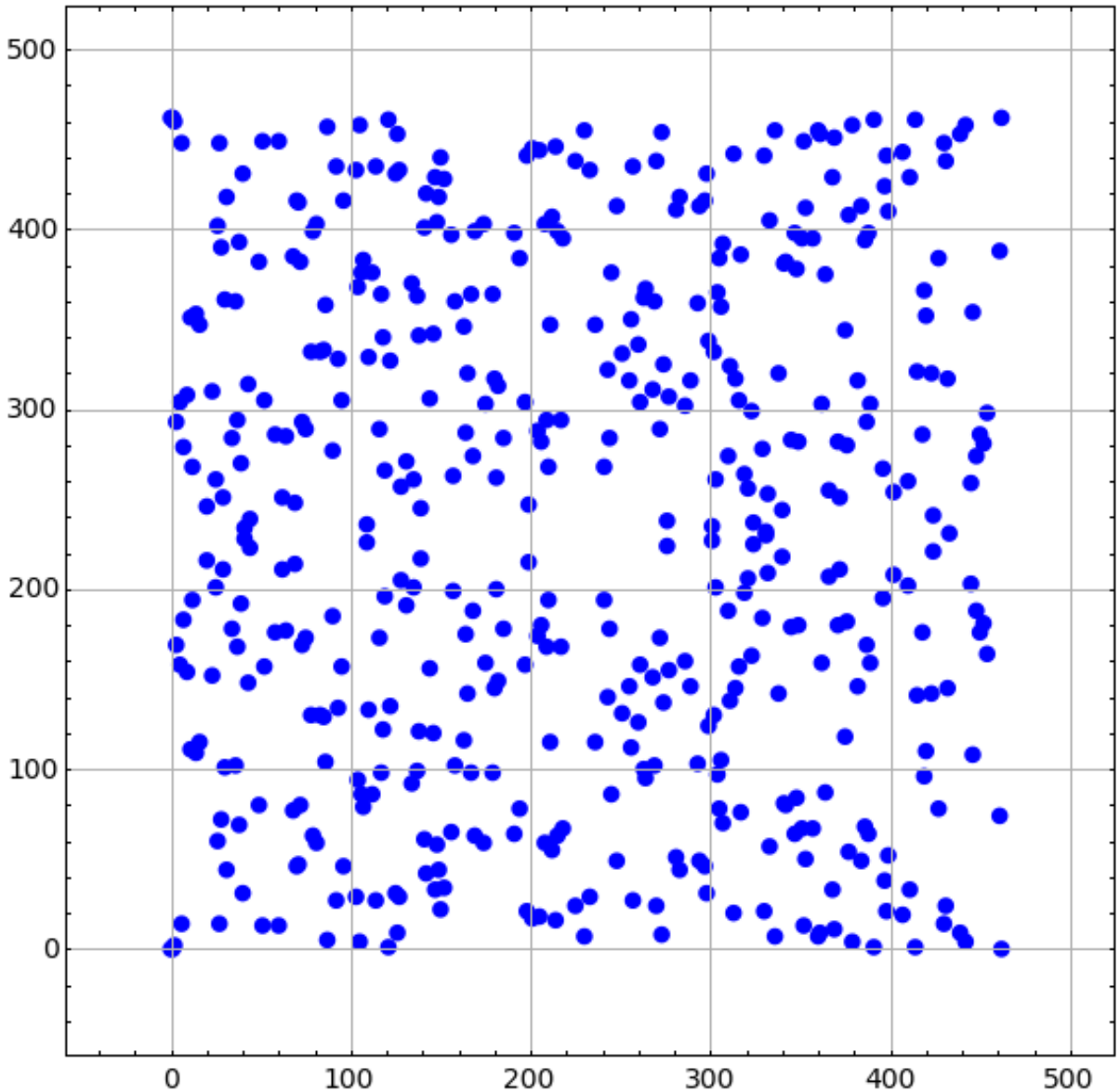
Courbes Elliptiques

- Domaine largement étudié par les mathématiciens du 20^{e} siècle sur $\mathbb{R}$ et $\mathbb{C}$.
- Soit $\mathbb{F}$ un **corps**. Une **courbe elliptique** est définie comme **l'ensemble des points** $(x, y) \in \mathbb{F}^2$ vérifiant l'équation

$$y^2 = x^3 + ax + b \ .$$

- On y ajoute en plus un point spécial $\mathcal{O}$ appelé **point à l'infini**.
- Dans ce cours, $\mathbb{F} = \mathbb{Z}_p$ avec $p > 3$ la plupart du temps.

Courbe Elliptique sur $\mathrm{GF}(p)$



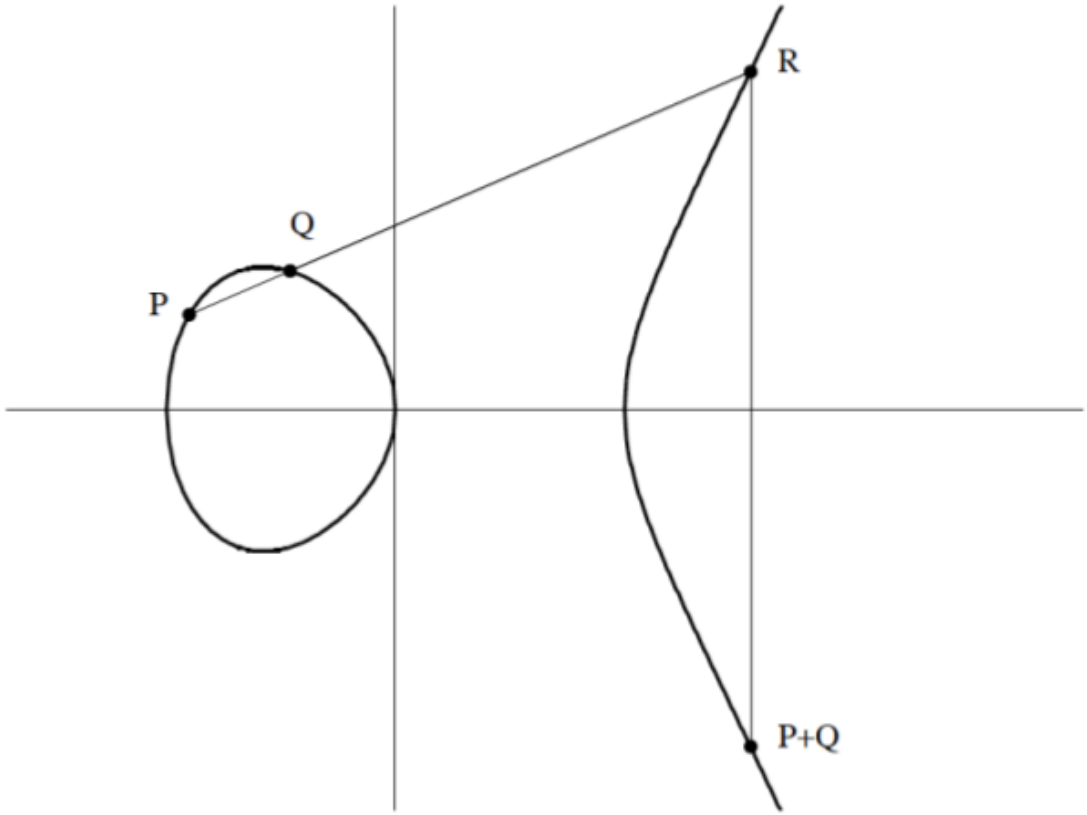
Exercice

Question

Quels sont les points sur la courbe $y^2 = x^3 + x + 2$ définie sur $\mathrm{GF}(5)$?

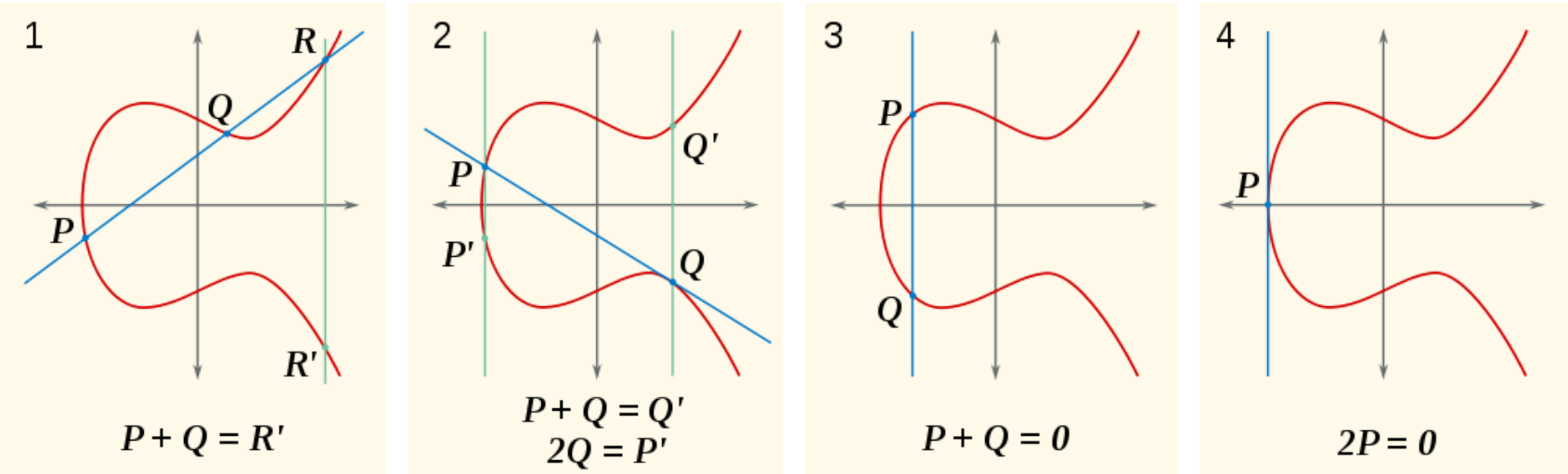
Addition de Points

- Une courbe elliptique forme **un groupe additif abélien**.
- Il nous faut une manière **d'additionner** les points.
- Ci-dessous, un exemple sur $\mathbb{R}$.



Source de l'illustration : http://en.wikipedia.org/wiki/Elliptic_curve

Addition de Points



Source de l'illustration : http://en.wikipedia.org/wiki/Elliptic_curve

Equation de la Droite

- Soit des points $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ et $x_P \neq x_Q$.
- L'équation de la droite qui passe par P et Q est :

$$y = \lambda x + h$$

avec λ la pente et h l'ordonnée à l'origine.

- On a

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

- $h = y_P - \lambda x_P$

Dérivation des Formules d'addition

- On cherche les trois points d'intersection entre la droite et l'équation de la courbe elliptique.
- On égalise donc ces deux équations

$$y^2 = x^3 + ax + b$$
$$y = \lambda x + h$$

- On doit trouver les trois solutions de l'équation

$$0 = x^3 - \lambda^2 x^2 + ax + (b + h)$$

- On note ces points $(x_1, y_1), (x_2, y_2), (x_3, y_3)$.
- On connait deux de ces trois points (x_P, y_P) et (x_Q, y_Q).

Dérivation des Formules d'addition

- L'équation
$$0 = x^3 - \lambda^2 x^2 + ax + (b + h)$$
est équivalente à l'équation
$$\begin{aligned} 0 &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - x^2(x_1 + x_2 + x_3) + x(x_1x_2 + x_2x_3 + x_1x_3) - x_1x_2x_3 \end{aligned}$$
- On sait que les termes en x^2 doivent être équivalents. On trouve donc
$$\lambda^2 = x_1 + x_2 + x_3$$
- Donc
$$x_3 = \lambda^2 - x_P - x_q$$

Dérivation des Formules d'addition

- Une fois la coordonnée x trouvée, la coordonnée y_R, résultat de l'addition, est le symétrique de ce qui sort de l'équation de la droite.
- $y_R = -\lambda x_3 - h = -\lambda x_3 - y_P + \lambda x_P = -y_P + \lambda(x_P - x_3)$.
- Dans le cas d'un **doublement de points**, seule l'équation de la pente change. On la trouve en dérivant l'équation de la courbe elliptique.

$$\frac{dE/dx}{dE/dy} = \frac{3x^2 + a}{2y}$$

- Quand évalué en (x_P, y_P), on obtient

$$\lambda = \frac{3x_P^2 + a}{2y_P}$$

Structure algébrique sur $\mathrm{GF}(p)$

- La courbe elliptique forme un **groupe additif**.
- L'élément neutre est $\mathcal{O}$.
- **L'inverse** d'un point (différent du point à l'infini) $P = (x, y)$ est $-P = (x, -y)$.
- **Attention :** cette formule n'est pas vraie sur tous les corps.

Addition de Points : Recette

Le résultat de $P + Q$ est

- $\mathcal{O}$ si $P = -Q$.
- P si $Q = \mathcal{O}$.
- Q si $P = \mathcal{O}$.
- $2P$ si $P = Q$. On applique la formule de **doublement de points**.
- Sinon, on applique la formule **d'addition de points**.

Formules d'Addition de Points sur $\mathrm{GF}(p)$

- Soient deux points $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ sur une courbe elliptique avec $x_P \neq x_Q$.
- $R = (x_R, y_R) = P + Q$ possède les coordonnées

$$\begin{aligned} x_R &= \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q \\ y_R &= -y_P + \left(\frac{y_Q - y_P}{x_Q - x_P}\right)(x_P - x_R) \end{aligned}$$

Formules de Doublement de Point sur $\mathrm{GF}(p)$

- Soit un point $P = (x_P, y_P)$ sur une courbe elliptique.
- $R = (x_R, y_R) = 2P$ possède les coordonnées

$$x_R = \left(\frac{3x_P^2 + a}{2y_P}\right)^2 - 2x_P$$

$$y_R = \left(\frac{3x_P^2 + a}{2y_P}\right)(x_P - x_R) - y_P$$

- Dans cette équation, a est un des **coefficients** de la courbe elliptique.

Attention

Tous les calculs doivent être effectués dans le **corps** sous-jacent $\mathbb{F}$.
Une division est donc une multiplication par l'inverse.

Exercice

Question

Calculez les opérations suivantes sur la courbe $y^2 = x^3 + x + 2$ définie sur $\mathrm{GF}(5)$:

- $(1, 2) + (4, 0)$
- $(1, 2) + (1, 3)$
- $(1, 2) + (1, 2)$
- $\mathcal{O} + (1, 2)$

Courbes Elliptiques sur $\mathrm{GF}(2^r)$

- Les courbes elliptiques peuvent aussi être définies sur $\mathrm{GF}(2^r)$.
- Les équations des courbes elliptiques y sont légèrement différentes.
- On considère souvent les deux formes suivantes :

$$y^2 + b_1 y = x^3 + a_1 x + a_0 \text{ avec } b_1 \neq 0$$
$$y^2 + xy = x^3 + a_2 x^2 + a_0 \text{ avec } a_0 \neq 0$$

- **Attention** Les formules d'addition et d'inversion de points sont **différentes**.
- En 2012, des attaques sur ces courbes rendent leur application à la cryptographie **douteuse**.

Théorème de Hasse

- Le théorème de Hasse garantit que n'importe quelle courbe elliptique définie sur un corps suffisamment grand aura un grand nombre de points.

Théorème (Hasse)

Si N est le nombre de points sur une courbe elliptique définie sur un corps fini à q éléments, alors N est borné par

$$(q+1) - 2\sqrt{q} \leq N \leq (q+1) + 2\sqrt{q}$$

Avantages des Courbes Elliptiques

- Le problème du **logarithme discret** (nommé **ECDLP**) peut être transposé sur une courbe elliptique : étant donné $R = xP$, calculer x.
- Les algorithmes les plus efficaces pour calculer le logarithme discret sur $\mathbb{Z}_p^*$ ne sont pas applicables dans le monde des courbes elliptiques.
- Ceci implique des **paramètres** beaucoup plus **petits**.

ECRYPT

The goal of ECRYPT-CSA (Coordination & Support Action) is to strengthen European excellence in the area of cryptology. This report [3] on cryptographic algorithms, schemes, keysizes and protocols is a direct descendent of the reports produced by the ECRYPT I and II projects (2004-2012), and the ENISA reports (2013-2014). It provides rather conservative guiding principles, based on current state-of-the-art research, addressing construction of new systems with a long life cycle. This report is aimed to be a reference in the area, focusing on commercial online services that collect, store and process the data.

Protection	Symmetric	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
Legacy standard level *Should not be used in new systems*	80	1024	160	1024	160	160
Near term protection *Security for at least ten years (2018-2028)*	128	3072	256	3072	256	256
Long-term protection *Security for thirty to fifty years (2018-2068)*	256	15360	512	15360	512	512

All key sizes are provided in bits. These are the minimal sizes for security.
Click on a value to compare it with other methods.

Recommended algorithms:
Block Ciphers: For near term use, AES-128 and for long term use, AES-256.
Hash Functions: For near term use, SHA-256 and for long term use, SHA-512 and SHA-3 with a 512-bit result.
Public Key Primitive: For near term use, 256-bit elliptic curves, and for long term use 512-bit elliptic curves.

Future algorithms (expected to remain secure in 10-50 year lifetime):
Block Ciphers: AES, Camellia, Serpent
Hash Functions: SHA2 (256, 384, 512, 512/256), SHA3 (256, 384, 512, SHAKE128, SHAKE256), Whirlpool-512, BLAKE (256, 584, 512)
Stream Ciphers: HC-128, Salsa20/20, ChaCha, SNOW 2.0, SNOW 3G, SOSEMANUK, Grain 128a

Groupe Additif vs Groupe Multiplicatif

	Groupe multiplicatif $\mathbb{Z}_p^*$	Groupe additif (courbe)
Opération	$a \cdot r$	$A + R$
Exp.	g^r	rG
Log	r étant donné g, g^r	r étant donné G, rG
Ordre	plus petit i tq $g^i = 1$	plus petit i tq $iG = 0$

Choix d'une Courbe Elliptique

- La courbe doit être **cryptographiquement** sûre.
- Elle doit avoir un point G d'ordre n (souvent premier)
- Le rapport entre le nombre de points N et n doit être petit, de préférence 1. $h = N/n$ est appelé le **co-facteur**.
- Trouver une bonne courbe est **compliqué**.
- Utilisez des courbes proposées dans des **standards** (SEC2, ANSI, ...)

ECDH

Question

Adaptez le protocole de Diffie-Hellman aux courbes elliptiques.

ECDH

1. Choisir une courbe elliptique cryptographiquement sûre avec N points et un point G d'ordre n premier.
2. Alice génère une valeur secrète $a \in \{1, \ldots, n-1\}$ uniformément au hasard, calcule $Y_a = aG$, et envoie Y_a à Bob via le canal authentique.
3. Bob génère une valeur secrète $b \in \{1, \ldots, n-1\}$ uniformément au hasard, calcule $Y_b = bG$, et envoie Y_b à Alice via le canal authentique.
4. Alice calcule $K = aY_b$ tandis que Bob calcule $K = bY_a$.
5. La clef secrète partagée est $\mathrm{KDF}(K)$.

Chiffrement d'El Gamal

On peut transcrire le chiffrement d'El Gamal sur une courbe elliptique.

1. Choisir une courbe elliptique cryptographiquement sûre et un point G d'ordre n.
2. **Clef privée** : $a \in \{1, \ldots, n-1\}$.
3. **Clef publique** : $A = aG$
4. Pour chiffrer un message M, on génère un nombre $k \in \{1, \ldots, n-1\}$ secret uniformément au hasard.
5. Le texte chiffré est la paire $(kG, M + [k(A)]_x)$, où $[.]_x$ retourne la coordonnée x du point de la courbe.

Question

Comment déchiffrer ?

ECDSA

Question

Adaptez le système de signatures DSA aux courbes elliptiques.

ECDSA paramètres

- On peut aussi transcrire l'algorithme de signature DSA sur une courbe elliptique.
- Utilisé dans bitcoin et dans le passport biométrique suisse.
  1. Choisir une courbe elliptique cryptographiquement sûre et un point G d'ordre n.
  2. Clef privée : $a \in \{1, \ldots, n-1\}$.
  3. Clef publique : $A = aG$

ECDSA signature

Pour signer un message M :

1. Génèrer un nombre $k \in \{1, \ldots, n-1\}$ secret uniformément au hasard.
2. Calculer $(x_1, y_1) = kG$.
3. $r = x_1 \bmod n$.
4. $s = \frac{H(M)+ar}{k} \bmod n$
5. La signature est (r, s) si $r \neq 0$ et $s \neq 0$. Sinon, recommencer.

ECDSA vérification

On vérifie une signature (r, s) de la manière suivante :

1. On vérifie que la clef publique $A \neq \mathcal{O}$, que A est bien sur la courbe et que $nA = \mathcal{O}$.
2. On vérifie que r et s sont des entiers dans $[1, n-1]$.
3. On calcule $u_1 = \frac{H(M)}{s} \bmod n$ et $u_2 = \frac{r}{s} \bmod n$.
4. On calcule $(x_1, y_1) = u_1 G + u_2 A$
5. On vérifie que $r = x_1 \bmod n$.

Solutions

Exercice points

Solution

Nous avons les points suivants : $\mathcal{O}, (1,2), (1,3), (4,0)$

Exercice calculs

Solution

- $(1,2)+(4,0)=(1,3)$.
- $(1,2)+(1,3)=\mathcal{O}$.
- $(1,2)+(1,2)=(4,0)$.
- $\mathcal{O}+(1,2)=(1,2)$.

Chiffrement d'El Gamal

Solution

On déchiffre un message (u, v) en calculant $v - [au]_x$.