

Les maths au secours des transactions bancaires

Mireille Fouquet

Université Paris Diderot



Journée de la fondation Sciences Mathématiques de Paris centre
28 septembre 2007

Achats sécurisés sur internet

The screenshot shows the 'Voyages-sncf.com' website interface. The browser address bar displays 'http://www.voyages-sncf.com/dynamic/_SvTermComm1Basket?_TMS=11907494553'. The page title is 'Votre Choix de voyage'. The navigation menu includes 'accueil', 'week-end', 'séjour', 'ski', 'France', 'hôtel', 'train', 'vol', 'voiture', 'loisirs+', 'promos', and 'ESPACE PRO'. A 'Mon Espace Client' section is visible with a 'Créer' button and a 'Mot de passe ?' link. The main content area shows a search result for 'PARIS -> BARCELONE' for 1 passenger, priced at 224.00 €. The itinerary details are as follows:

PARIS -> BARCELONE		1 passager	224.00 €
Aller :	20h32 PARIS AUSTERLITZ 08h24 BARCELONA FRANCA	00477 2e classe Cabine T4 (4 lits)	Vendredi 28 Septembre
1e Passager (26 à 59 ans)	LOISIR Aller-retour obligatoire. Echangeable avant le départ. Remboursement sous conditions avant et après départ.	Voiture 78 - Place 55 Supérieur	
Retour :	21h05 BARCELONA FRANCA 09h00 PARIS AUSTERLITZ	00475 2e classe Cabine T4 (4 lits)	Dimanche 30 Septembre
1e Passager (26 à 59 ans)	LOISIR Aller-retour obligatoire. Echangeable avant le départ. Remboursement sous conditions avant et après départ.	Voiture 78 - Place 32 Inférieur	

Buttons: Supprimer

TOTAL 224.00 €

Ajouter: Un autre billet, Une carte de réduction SNCF, Un hôtel

Problème : La SNCF et moi ne partageons pas un même secret pour chiffrer et déchiffrer nos communications.

Motivations

Protocole de Diffie-Hellman : Soit G un groupe cyclique à n éléments de générateur g .

Mireille Fouquet	transmission en clair	Voyages-sncf.com
choisit $a \in [1, n[$ calcule $K_A = g^a$	$\begin{array}{c} \xrightarrow{K_A} \\ \xleftarrow{K_B} \end{array}$	choisit $b \in [1, n[$ calcule $K_B = g^b$
calcule $K_{AB} = K_B^a$		calcule $K_{AB} = K_A^b$

Secret commun : $K_{AB} = g^{ab}$

Problème du logarithme discret = calculer x en connaissant g et g^x .

Exemple : Dans $\mathbb{Z}/11\mathbb{Z}$, si on pose $g = 2$ et $x = 8$ alors $g^x = 3 \pmod{11}$.

Comment retrouver x à partir de 2 et de 3 ?

WANTED

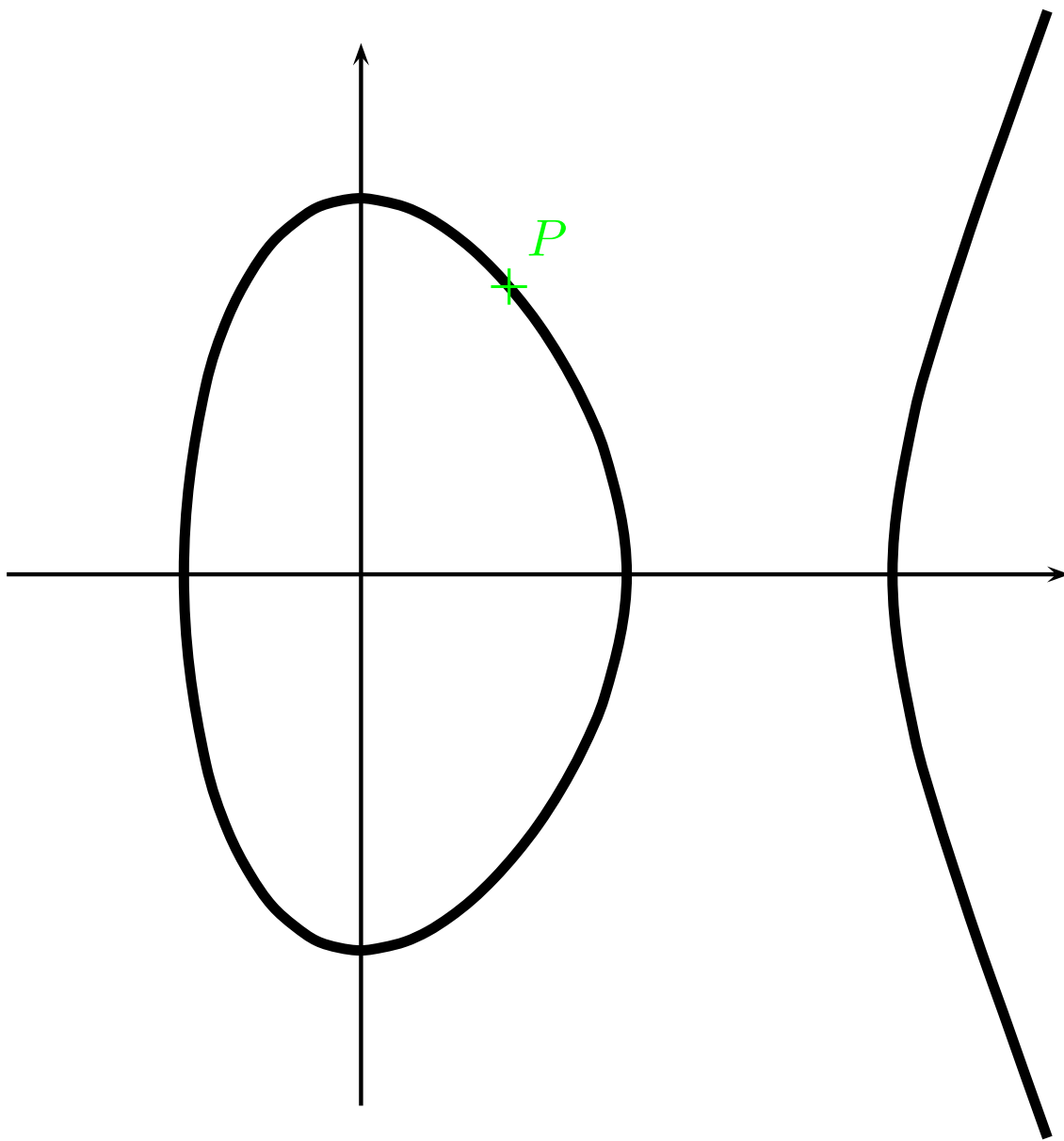
On cherche un groupe G tel que

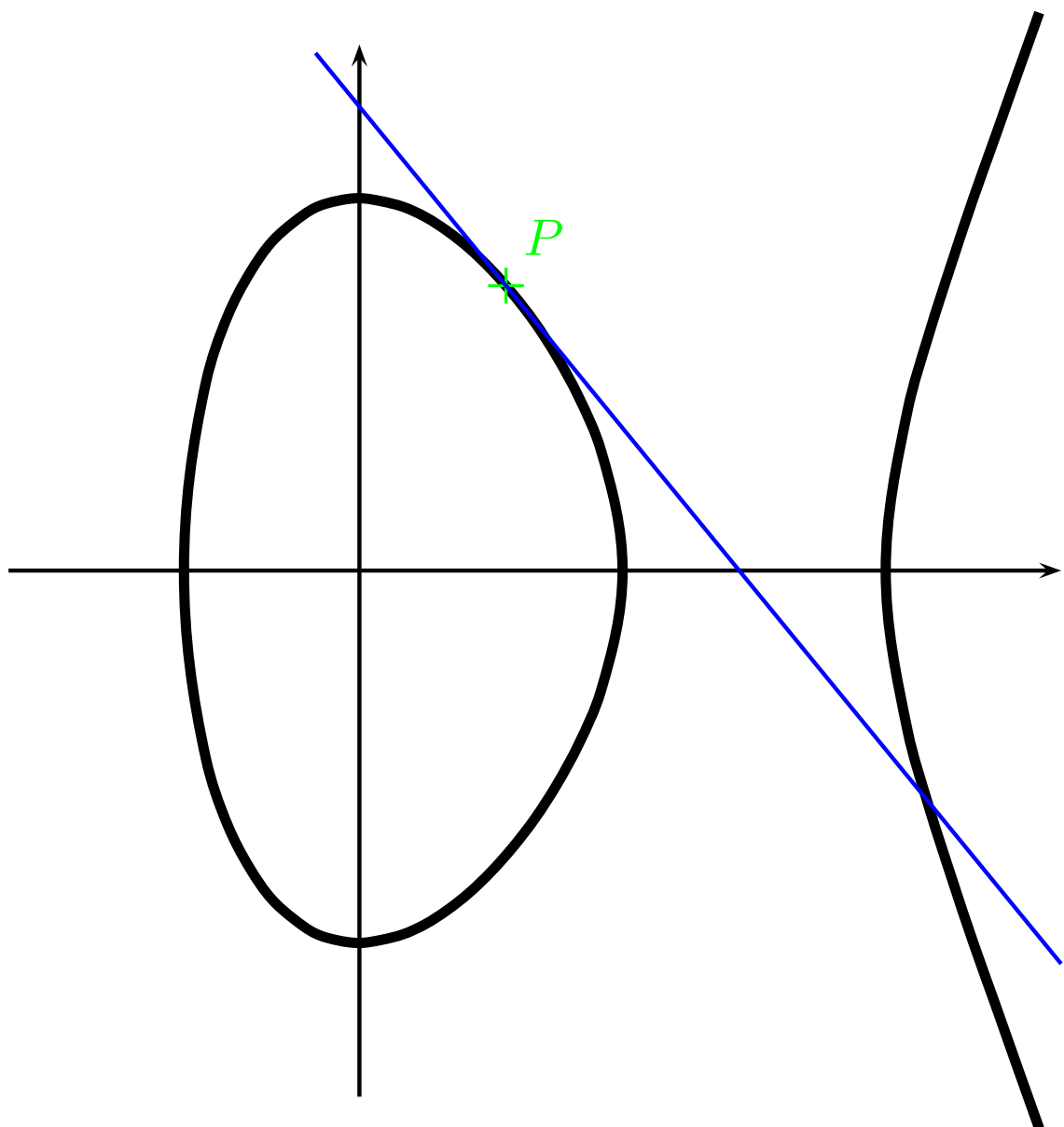
- calculer dans le groupe est simple ;
- résoudre le problème du logarithme discret est difficile dans le groupe.

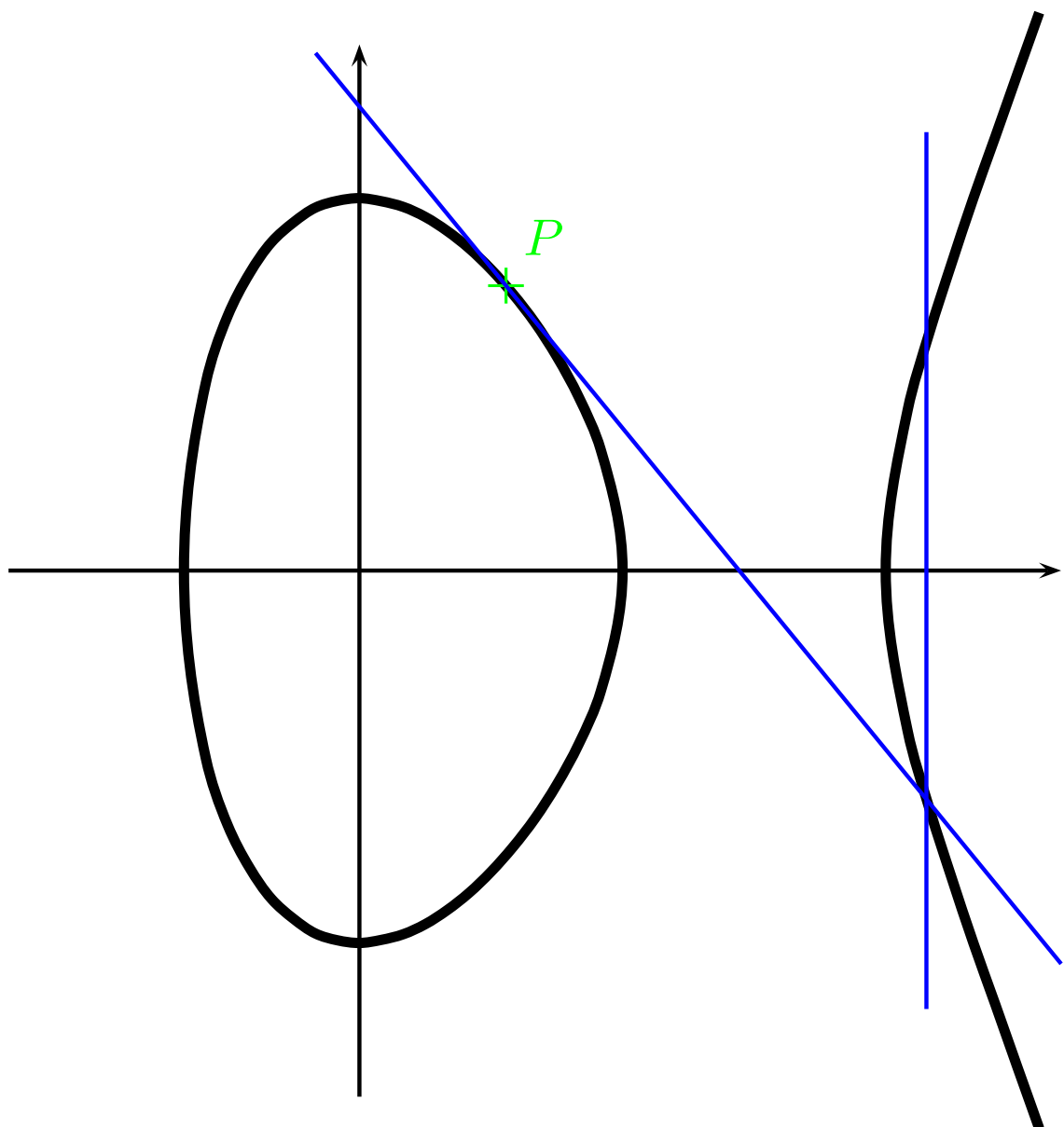
Candidat naturel : Groupe multiplicatif des corps finis (ex : $(\mathbb{Z}/11\mathbb{Z})^*$).

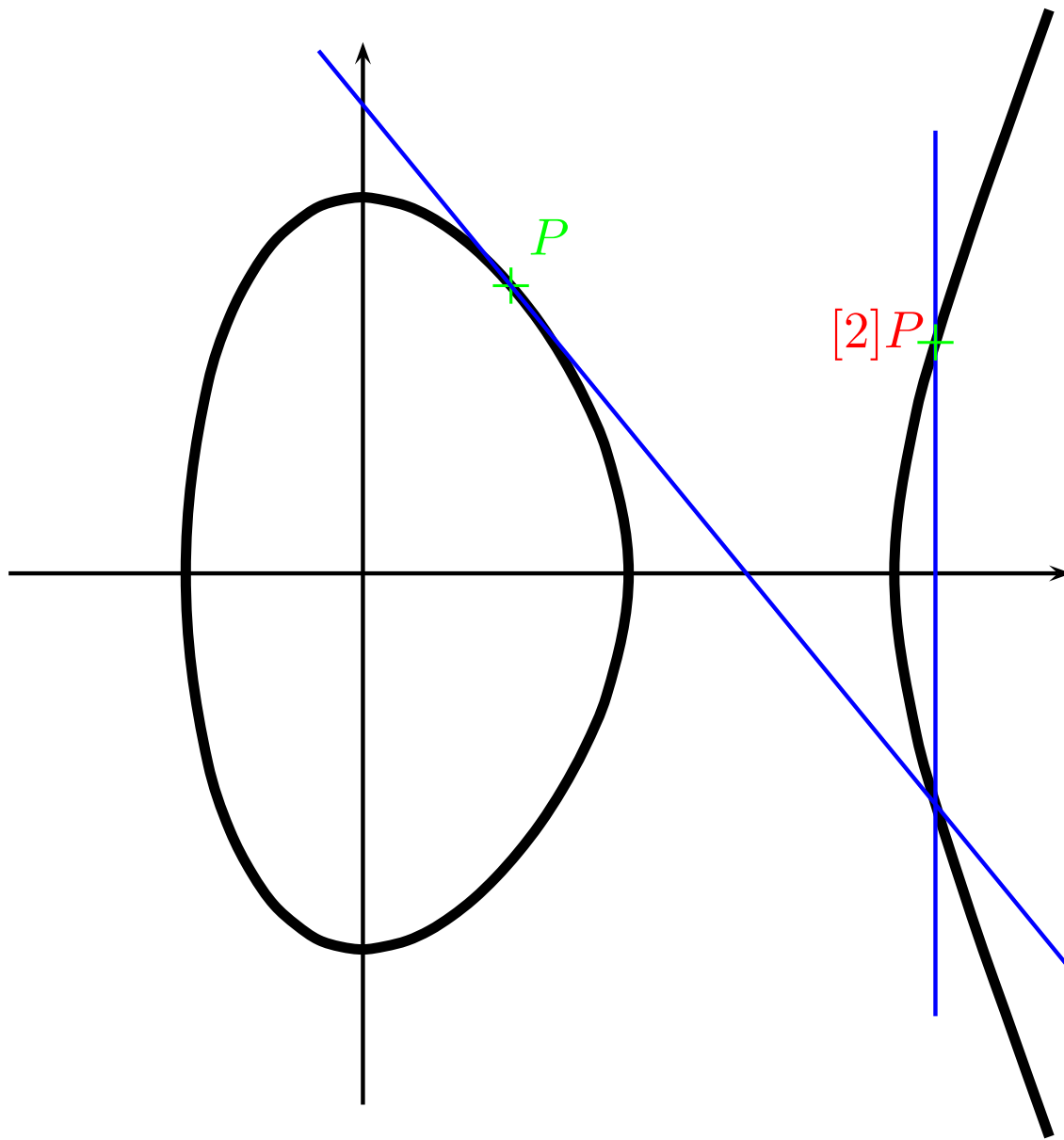
Utilisation en milieu contraint (carte à puce, organisateur électronique, téléphone portable, ...) : Nécessité d'un objet mathématique petit avec un même niveau de sécurité.

Bon candidat : Courbes elliptiques définies sur un corps fini.









Loi de groupe simple + pas d'attaque générale connue pour le log discret.

Axes de recherche

- Calculer le nombre de points d'une courbe elliptique sur un corps fini de manière efficace
- Vérifier l'invulnérabilité d'une courbe elliptique donnée aux attaques connues
- Étudier l'ensemble des invariants des courbes elliptiques afin de trouver de nouvelles attaques