1 Slide 1

- **introduction** : la factorisation : la **décomposition** en facteurs premiers
- courbes elliptiques : ensembles → munis d'une structure de groupe → méthode de factorisation
- méthode inventée en 1985 par Lenstra ; reste la meilleure pour les entiers entre 10^6 et 10^{30}
- **notation** : on peut considérer une même courbe sur différents corps
- **point à l'infini** ← déf générale : cubique définie dans le plan projectif
- **caractéristique première avec** 6 ← changements de variable pour se ramener à la forme réduite de Weierstraß réduite : $Y^2Z+a_1XYZ+a_3YZ^2 = X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$ (forme de Weierstraß générale) → changements de variable : $Y \leftarrow (Y-\frac{1}{2}(a_1X+a_3))$ et $X \leftarrow (X-\frac{a_1^2+4a_2}{12}Z)$

2 Slides 2 et 2 bis

- s'appelle la loi de la **sécante-tangente**
- permet de définir $\mathbf{P} * \mathbf{Q}$: 3e point d'intersection
- **courbe non singulière** ← $P * P$
- ces propriétés découlent du fait qu'un **polynôme de degré** 3 admet au plus 3 racines dans le corps $\mathbb{K}$; il admet 2 racines, il en admet forcément 3
- l'inverse est calculé dans $\mathbb{K}$ → importance du **corps** pour l'inversibilité : qd on ne pourra pas calculer l'inverse on aura des **facteurs** de N
- l'inverse est, en pratique, calculé avec **Bezout**

3 Slide 3

- on a besoin de connaitre un **majorant du Card de** E → Lagrange : point P tq $kP = \mathcal{O}$
- tous les corps finis $\mathbb{F}_p$ sont **isomorphes**
- Hasse : meilleure approximation possible ; Deuring a montré que **toutes les valeurs sont possibles**
- si l'ordre de P divise N alors il divisera k et donc $\mathbf{kP} = \mathcal{O}$

4 Slide 4

- j'ai programmé cet algorithme
- a et b **paramètres** : ds mon prog a est incrémenté de 30 en 30
- $\Delta \wedge N$ est calculé avec **Bezout**
- on suppose p **premier** (donc N non premier)
- **n'aboutit pas forcément** (si N est premier)
- $P = (1, 1)$: choix arbitraire

5 Slide 5

- ds l'**exponentiation rapide** : $P' + P'' = \mathcal{O}$
- les égalités (pour $P + Q = \mathcal{O}$) sont des **congruences** modulo p
- les PGCD sont calculés avec l'algorithme de Bezout
- le facteur trouvé n'est **pas forcément premier** (il est simplement divisible par p)
- **on continue de factoriser** les facteurs trouvés
- la méthode **n'aboutit donc jamais** (lorsque N est premier)
- temps moyen : $O(\mathrm{e}^{(1+\varepsilon)\ln N \ln\ln N})$
- concl : la factorisation est un pb NP-complet
- résultats

6 Slide 6

- c'est avec $a = \ldots$ et $B = \ldots$ que j'ai trouvé un facteur de $\ldots$ en $\ldots$