La factorisation des entiers : une décomposition

La factorisation d'entiers en produit de nombres premiers est une décomposition longue à réaliser – il n'existe aucun algorithme polynômial pour la réaliser – et c'est sur cette difficulté même que se fonde la plupart des systèmes cryptographiques actuels. La méthode proposée par Lenstra en 1985, à laquelle je me suis intéressé, reste l'une des plus performantes. Elle a marqué une avancée importante dans la recherche de l'amélioration de la complexité des algorithmes de factorisation.

Après avoir fait des recherches – principalement sur internet – concernant les aspects théoriques de cette méthode, je l'ai implémentée en C++ (cf. verso), ce qui m'a permis d'obtenir des résultats effectifs.

Définition des courbes elliptiques

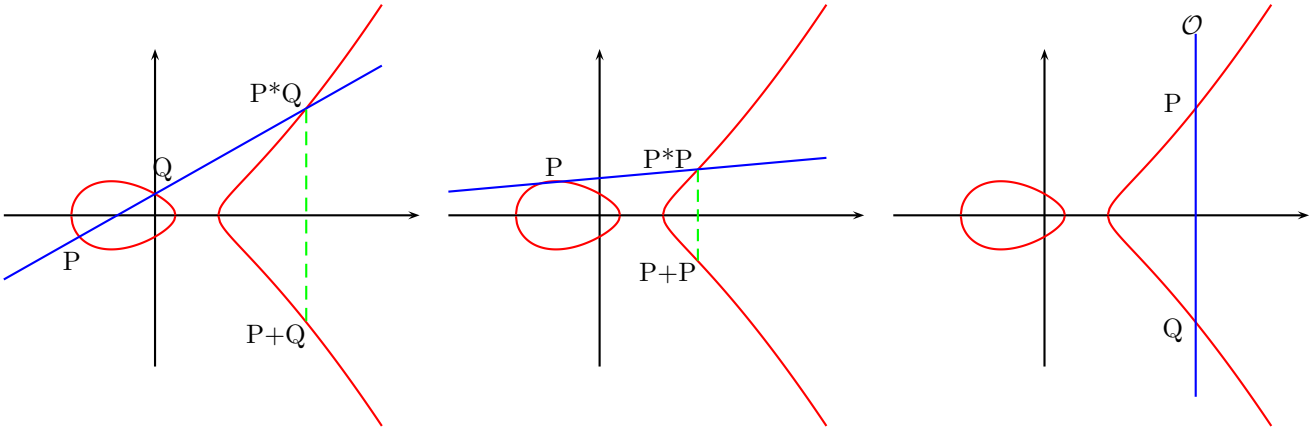
Une *courbe elliptique* $E(\mathbb{K})$ définie sur un corps $\mathbb{K}$ de caractéristique différente de 2 ou 3 est un ensemble défini par :

$$E_{a,b}(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \ / \ y^2 = x^3 + ax + b\} \cup \{\mathcal{O} = (0, 1, 0)\}$$

Structure de groupe

La loi de composition interne $*$ est définie par : $R = P * Q$ ssi R est le troisième point d'intersection de (PQ) avec la courbe ($R = \mathcal{O}$ si (PQ) est "verticale" et (PQ) est la tangente en P si $P = Q$).

La loi de groupe $+$ est alors définie par : $P + Q = \mathcal{O} * (P * Q)$.



$(E, +)$ ainsi défini est un groupe abélien de neutre $\mathcal{O}$.

Théorème de Hasse, B-superlissité

Le *théorème de Hasse* : la cardinalité $\#E(\mathbb{F}_p)$ vérifie : $|p+1-\#E(\mathbb{F}_p)| \leq 2\sqrt{p}$.

$N = \prod_{i=1}^{m} p_i^{\alpha_i}$ est dit *B-superlisse* ssi : $\forall i \in [\![1,m]\!], p_i^{\alpha_i} \leq B$.

Méthode de Lenstra pour la factorisation

- les vérifications préliminaires : $N \wedge 6 = 1$, $P = (1,1) \in E_{a,b}$, $\Delta \wedge N = 1$;
- la détermination de k tel que $kP = \mathcal{O}$ dans $E_{a,b}(\mathbb{Z}/p\mathbb{Z})$;
- explication de la détection possible d'un facteur de N (non inversible dans $\mathbb{Z}/N\mathbb{Z}$) lors du calcul de λ.

Résultats de l'implémentation

L'implémentation a été réalisée à l'aide de Visual C++ 6.0 et testée sur un Pentium 4 1,5 GHz avec 256 Mo de RAM. Elle a en particulier permis de trouver, en 9 minutes seulement, un facteur premier d'un entier produit de trois facteurs premiers de 8 chiffres.

Des difficultés techniques ont dû être surmontées, en particulier la réalisation d'une classe supportant les opérations dans les courbes elliptiques ; le programme utilise entre autres l'algorithme d'Euclide avec obtention des cœfficients de Bezout (pour l'inversion dans $\mathbb{Z}/n\mathbb{Z}$), l'exponentiation rapide et la gestion d'entiers de taille arbitraire (supérieure à 32 bits).

Bibliographie

- Site *Certicom*. `http://www.certicom.com/resources/ecc/ecc.html`.
- François Arnault. *Théorie des nombres et cryptographie*. Cours de DEA, Université de Limoges, mars 2000. `http://www.unilim.fr/laco/perso/francois.arnault`.
- Johannes Buchmann. La factorisation des grands nombres. *Pour la science* 251, pages 88–96, septembre 1998.
- Thomas Cormen, Charles Leiserson, et Ronald Rivest. *Introduction à l'algorithmique*. Dunod, 1994.
- Marc Joye. *Une introduction élémentaire à la théorie des courbes elliptiques*. Technical report, Université catholique de Louvain, juin 1995. `http://www.dice.ucl.ac.be/crypto`.
- Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. Thèse, LIX – CNRS, juin 1997. `http://www.medicis.polytechnique.fr/~lercier/preprints`.
- Douglas Stinson. *Cryptographie – Théorie et pratique*, chapitre 5, pages 159–170. International Thomson publishing, 1995.