Arithmétique et Cryptographie

Jean-Louis Nicolas

Université Claude Bernard (Lyon)

Les méthodes récentes de cryptographie (c'est-à-dire de transmission secrète des messages) utilisent des propriétés arithmétiques. L'une d'elles, la méthode RSA, est basée sur le fait qu'il est relativement facile de construire de grands nombres premiers, mais si l'on fait le produit $n = p \times q$ de deux tels nombres on ne sait pas retrouver à partir de n seulement les facteurs initiaux p et q. Les courbes elliptiques, essentiellement les courbes d'équation $y^2 = x^3 + ax + b$, jouent aussi un certain rôle dans cette affaire. La plupart des algorithmes décrits sont probabilistes, mais sont en pratique performants.

Premier exposé : **Les algorithmes et les principaux protocoles de cryptographie.**

Il sera rappelé comment on peut calculer les principales fonctions arithmétiques : la relation de Bézout, l'algorithme des puissances, le symbole de Legendre, l'algorithme LLL, etc.... Nous décrirons aussi quelques protocoles de cryptographie : RSA, Diffie et Hellman, le sac à dos, jouer à pile ou face par téléphone.

Deuxième exposé : **les tests de primalité.**

Dans cet exposé, nous introduirons les courbes elliptiques, nous montrerons comment construire de grands nombres premiers, et décrirons les principales méthodes pour prouver qu'un nombre donné est premier.

Troisième exposé : **Les méthodes de factorisation et le logarithme discret**.

Etant donné un nombre déclaré non premier par un algorithme décrit dans le précédent exposé, comment trouver ses facteurs premiers? Depuis une trentaine d'années, différentes méthodes ont été découvertes , beaucoup plus efficaces que la division par les nombres premiers successifs.

Soit P un grand nombre premier. On sait que le groupe $(\mathbb{Z}/P\mathbb{Z})^*$ est cyclique, autrement dit il existe un générateur g tel que les ensembles

$$\{1, 2, \ldots, P-1\} \text{ et } \{g \bmod P, g^2 \bmod P, \ldots, g^{P-1} \bmod P\}$$

coïncident. Tout nombre a, $1 \leq a \leq P-1$ s'écrit donc de façon unique $a \equiv g^x \pmod{P}$, avec $1 \leq x \leq P-1$. On appelle x le logarithme discret en base g de a. Cette fonction est utilisée en cryptographie, et l'on verra que les méthodes de calcul du logarithme discret sont voisines des méthodes de factorisation.

Les livres conseillés sont les livres de H. Cohen ([1]) pour la partie mathématique, et ceux de G. Robin ([2]) et B. Schneier ([3]) pour la cryptographie.

Références

[1] H. Cohen. *A course in algorithmic algebraic number theory*, Graduate Texts in Mathematics vol. 138, Springer-Verlag 1993.

[2] G.Robin. *Algorithmique et cryptographie*, Mathématiques et Applications vol. 8, Ellipses, Paris, 1991.

[3] B. Schneier. *Applied Cryptography*, 2nd ed., J.Wiley and sons, New-York, 1996.