Théorie Algorithmique des Nombres

Méthodes sous-exponentielles

David Kohel

02/11/2020

Méthodes sous-exponentielles

L'idée: On veut comprendre la structure du groupe $(\mathbb{Z}/N\mathbb{Z})^*$. Si N est composé, avec $N=pq$, où $\text{pgcd}(p,q)=1$, on a

$$(\mathbb{Z}/N\mathbb{Z})^* \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$$

En particulier, si N est impair,

$$(\mathbb{Z}/N\mathbb{Z})^*[2] \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^*[2] \times (\mathbb{Z}/q\mathbb{Z})^*[2]$$

$$\| \qquad\qquad \cup \qquad\qquad \cup$$

$$\{a \in (\mathbb{Z}/N\mathbb{Z})^* : a^2=1\} \qquad \{\pm 1\} \qquad \{\pm 1\}$$

et le cardinal de $(\mathbb{Z}/N\mathbb{Z})^*[2]$ est plus grand que $2=|\{\pm 1\}|$, en particulier il y a au moins

$$4=|\{\pm 1\}\times\{\pm 1\}|$$

éléments. Deuxièmement on a beaucoup d'éléments "petits":

$$\{2,3,5,7,\dots,p\} \subseteq (\mathbb{Z}/N\mathbb{Z})^*$$

qui sont des générateurs distingués

On peut facilement reconnaître un grand nombre d'éléments de $(\mathbb{Z}/N\mathbb{Z})^*$ par la factorisation d'un représentant $a \in \mathbb{Z}$:

$$\pm a = 2^{e_1} 3^{e_2} 5^{e_3} \cdots p^{e_n}.$$

On va utiliser ces factorisations pour déterminer :

- relations (multiplicatives) entre les générateurs :

$$\pm 1 = 2^{e_1} 3^{e_2} \cdots p^{e_n} = (-1)^{e_0}$$

On dit que $(e_0, e_1, e_2, \ldots, e_n) \in \mathbb{Z}^{n+1}$ est un vecteur de relations.

- On a un sous-module $M \subseteq \mathbb{Z}^{n+1}$ de relations tel que l'homomorphisme

$$\begin{aligned} M \subseteq \mathbb{Z}^{n+1} &\xrightarrow{\pi} (\mathbb{Z}/N\mathbb{Z})^* \\ (e_0, e_1, \ldots, e_n) &\longmapsto (-1)^{e_0} 2^{e_1} \cdots p^{e_n} \end{aligned}$$

a noyau $M = \ker(\pi)$.

Ensuite :

- On va construire $L \subseteq \mathbb{Z}^{n+1}$ tel que

$$M \subseteq L \subseteq \mathbb{Z}^{n+1}$$

avec $L/M \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^*[2]$, ce qui permet de factoriser N.