Une démonstration informelle de ma version C de l'implantation GP de Sylvain Duquesne et Christophe Doche de SEA.

Fonction L d'une courbe elliptique

Soit E une courbe elliptique défini sur $\mathbb{Z}$ par une équation de Weierstrass $Y^2 + \mathbf{a}_1 XY + \mathbf{a}_3 Y = X^3 + \mathbf{a}_2 X^2 + \mathbf{a}_4 X + \mathbf{a}_6$. Pour $Re(s) > \frac{3}{2}$ la fonction L de E est donnée par le produit eulérien:

$$L(E,s) = \prod_p \frac{1}{1 - a_p p^{-s} + \varepsilon(p) p^{1-2s}}$$

où

- $\varepsilon(p)$ vaut 1 si p a bonne réduction et 0 sinon.
- $a_p = p + 1 - |E(\mathbb{F}_p)|$
- $|a_p| < 2\sqrt{p}$ (Hasse-Weil)

Algorithmes pour calculer a_p

- Sommes de Jacobi $O(p \log(p)^2)$
- Shanks-Mestre $O(p^{1/4} \log(p)^2)$
- Schoof $O(\log(p)^8)$ (déterministe)
- SEA (Schoof-Elkies-Atkin) $O(\log(p)^6)$ (probabiliste)
- Algorithmes spécifiques pour certains type de courbe, par exemple à multiplication complexe.

SEA dans PARI/GP 2.4.3

Essentiellement une traduction en C de l'implantation GP de Sylvain Duquesne et Christophe Doche de SEA pour le project AREHCC, qui lui-même est inspiré de la thèse de Reynald Lercier.

Accessible sous GP via la fonction ellap().

Nécessite l'installation du paquet seadata contenant les polynômes modulaires.

Principe de SEA

Pour un petit nombre premier ℓ on utilise l'équation modulaire de niveau ℓ pour déterminer les classes de congruences acceptable de a_p modulo ℓ. Lorsque que suffisament de congruences sont connus, on determine les solutions possibles par restes chinois et l'on trouve la vraie valeur de a_p par un algorithme "pas de bébé-pas de géant".

Temps (sur mon portable) pour la courbe $Y^2 = X^3 + X + 17$.

taille de p	temps
100bit	0.22s
150bit	1.5s
200bit	6s
250bit	16s
300bit	17s
350bit	58s
400bit	2min 44s
450bit	5min 17s
500bit	10min
600bit	20min
700bit	31min