Chers Gaudry et Harley,

1 Utilisation de l'AGM pour le calcul de $E(\mathbf{F}_{2^n})$

Si K est un corps p-adique de corps résiduel k, d'uniformisante π, et si $a_0, b_0 \in O_K$ sont tels que $a_0/b_0 \mod 8\pi$, la suite arithmético-géométrique définie par les formules

$$(a_{n+1}, b_{n+1}) = ((a_n + b_n)/2, \sqrt{a_n b_n})$$

converge (la racine carrée étant convenablement choisie, voir ma note aux CRAS avec Henniart pour les détails.)

Si E_n est la courbe $y_n^2 = x_n(x_n - a_n^2)(x_n - b_n^2)$, le passage de (a_n, b_n) à (a_{n+1}, b_{n+1}) s'interprète comme une isogénie f de degré 2 de E_{n+1} sur E_n, qui vérifie $f^*(dx_{n+1}/y_{n+1}) = dx_n/y_n$.

Mais les conditions sur a et b signifient que E_0 est une courbe de Tate, i.e. la réduction est multiplicative.

Néanmoins, lorsque $k = \mathbf{F}_{2^d}$, et lorsque $\pi = 2$, cet algorithme me semble pouvoir être utile pour calculer le nombre de points de $E \mod k$ d'une courbe elliptique E *ordinaire* définie sur K.

Soit en effet E une courbe elliptique définie sur K, à multiplications complexes par un corps L où 2 est décomposé. Si F est le Frobenius, d'image λ dans L, on a $F^*(\omega) = \lambda\omega$, où ω est une différentielle de première espèce de E (par exemple $\omega = dx/y$ si E est donnée par une équation de Weiertrass), L étant plongé de façon convenable dans $\overline{K}$.

Par ailleurs, il existe un modèle de E de la forme $y^2 = x(x-a^2)(x-b^2)$, avec $a/b \equiv 1 \mod 4$. En effet, on part d'un modèle minimal de E sur O_K; comme E a réduction ordinaire, elle possède un unique point d'ordre 2 dont l'abcisse n'est pas dans O_K - c'est celui qui se réduit en le noyau du Frobenius. Ce point est donc rationnel sur K, et on obtient une équation de la forme voulue en le ramenant à être le point $(0, 0)$. Notons que a et b sont éventuellement dans une extension quadratique de K, mais ce n'est pas grave: au pas suivant, on retrouve en effet une courbe E_1 d"equation $y^2 = x(x-a_1^2)(x-b_1^2)$, a_1 et b_1 dans K, et le calcul de a_1 et b_1 peut se faire en restant dans K (voir la note citée ci-dessus).

Au bout de d itérations, on trouve une courbe E_d d'équation $y^2 = x(x - a_d^2)(x - b_d^2)$ isomorphe à E. Le (dual du) Frobenius est alors égal à a/a_d, donc sa trace à

$$a/a_d + 2^d a_d/a.$$

On obtient ainsi le nombre de points de $E(\mathbf{F}_{p^d})$.

Si à présent on part d'une courbe elliptique ordinaire F définie sur k, le problème est donc de trouver le relèvement canonique de F. On peut employer, comme vous le faites, la méthode de Newton appliquée à $\Phi(j, j')$.

Mais en fait, l'algorithme arithmético-géométrique permet également de le faire: on remonte la courbe en une courbe E_0 sur K, que l'on écrit sous la forme $y^2 = x(x - a_0^2)(x - b_0^2)$. On applique l'algorithme arithmético-géométrique, d'où une suite $E_0, E_1, \ldots$ de courbes d'équations $y^2 = x(x - a_n^2)(x - b_n^2)$ définies sur K. Les a_n et b_n ne convergent pas, contrairement au cas des courbes de Tate de la note avec Henniart, mais les courbes $E_0, E_d, E_{2d}, \ldots$ convergent vers le relévement canonique de la courbe initiale (ou, si l'on préfère, leurs invariants modulaires convergent vers le rel´evement canonique de l'invariant modulaire de F). Mais la convergence est linéaire, au lieu d'être quadratique comme par Newton.

2 Courbes de genre 2

Une méthode analogue à celle du paragraphe précédent permet de trouver le nombre de points d'une courbe ordinaire de genre 2 sur $k = \mathbf{F}_{2^d}$ (ou plus précisément d'en calculer le Frobenius).

Si E est une courbe de genre 2 ordinaire sur k, on peut la remonter sur K (avec les notations du paragraphe précédent) en une courbe d'équation $y^2 = f(x)$, où $f \equiv f_3(x)^2 \mod 2$, f_3 de degré 3 et séparable.

Ici, c'est l'algorithme décrit dans l'article que Bost et moi avions écrit dans la Gazette qu'on applique. En p-adique, cet algorithme converge dans le cas des courbes de Mumford, mais, comme pour l'AGM, dans le cas 2-adique, bien qu'il ne converge pas, il permet de calculer d'une part le relèvement canonique de la courbe, d'autre part son Frobenius.

On écrit $f = p_1 p_2 p_3$, où p_1, p_2 et p_3 sont des carrés $\mod 2$, on calcule $q_1 = p_2' p_3 - p_3' p_2$, etc, comme dans l'article en question, et on itère (À noter que les p_i ne sont en général pas dans $K[x]$, mais dans une extension de degré 2 ou 3 de K). En itérant, on obtient un algorithme *linéaire* de convergence vers le relèvement canonique de C.

Ensuite, on fait comme dans la section précédente: si C_0 définie sur K est à multiplications complexes et ordinaire, l'algorithme répété d fois donne une courbe C_d qui lui est isomorphe; on cherche la fonction homographique $x \mapsto h(x) = (ax + b)/(cx + d)$ et λ tels que $(x, y) \mapsto (h(x), \lambda y/(cx + d)^3)$ soit un isomorphisme de C_0 sur C_d. Au signe près, le (dual du) Frobenius agissant sur les formes différentielles régulières a alors comme matrice

$$M = \frac{ad - bc}{\lambda} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Par suite, si $N = M + 2^d M^{-1}$, le polynôme caractéristique du Frobenius est $x^2 P(x + 2^d/x)$, où P est le polynôme caractéristique de la matrice N.

Bonnes vacances,
J-F. Mestre.