xの次数が偶数の時の超楕円曲線のヤコビアンの加法アルゴリズムについて

綱友之(早稲田大学)

- **本講演では、有限体上の方程式**

$$y^2 = x^{2g+2} + \ldots + a_{2g+2}$$

で定義される超楕円曲線のヤコビアンの加法について考察する。

Outline

- **準備**
- **「加法アルゴリズム」の意味**
- **加法アルゴリズムの構成**
- **具体例**

今回の超楕円曲線

- **定義式**: $y^2 = x^{2g+2} + \ldots + a_{2g+2}$ over $\mathrm{F_q}$
- **貼り合わせ**

$$v^2 = a_{2g+2}u^{2g+2} + \ldots + 1$$

$$u = \frac{1}{x}, v = \frac{y}{x^{g+1}}$$

- **無限遠点**: O, O' ($\mathrm{F_q}$-rational points)

超楕円曲線のヤコビアン

- **群構造**: $Div^0(C)/\sim$ (~ **は線形同値**)

- **元**: D=(**有限点の形式和**)+aO+bO’
  D**が** F_q **の絶対ガロア群の任意の元の作用で不変ならば、**D**は** F_q **有理点であるという。**

regulator

- $O-O'$: F_q **有理点**
  $O-O'$ **の位数を(曲線の)**regulator**と呼ぶ。**

Regulator**を求めるアルゴリズムとして、連分数と類似の理論をもちいたものがある。**
(ex Berry)

半被約因子と被約因子

- D: F_q **有理点**
  D**が** $P_1+\ldots+P_n+aO-(a+n)O'$**という形の時**
  D**は半被約因子であると呼ぶ。**

  D**が**

  $$P_1+P_2+\ldots+P_g+aO-(a+g)O'$$

  という形の時D**は被約因子であると呼ぶ。**

- F_q有理点は全て被約因子としてよい。
- **被約因子の表現の一意性:成立しない**

(例)

$$y^2 = x^6 + x^3 - 1 \mod 7$$

$$div(y - x^3) = P_1 + P_2 + P_3 - O - 2O'$$

$$P_1 + P_2 - O - O' \sim -P_3 + O'$$

Mumford representation

- D: F_q**有理点**
  D= $P_1 + \ldots + P_n + aO - (a+n)O'$ $\quad P_i = (x_i, y_i)$
  $P_1 + \ldots + P_n$ **は**

$$\left(u(x) = \prod_{i=1}^{n} (x - x_i),\ y - v(x) \right)$$ **という組で表現可能**

$$D = [(u,v), aO, -(a+2)O']$$ **と表せる。**

加法の意味

- $D_1 = [(u_1, v_1), a_1 O, b_1 O']$

  $D_2 = [(u_2, v_2), a_2 O, b_2 O']$

  この時 $D_1 + D_2$ **と同値な点**

  $D_3 = [(u_3, v_3), a_3 O, b_3 O']$ **を求めよ。**

加法アルゴリズム

- Composition part

Step1,Use the Euclidean algorithm to find polynomials

$$d_1, e_1, e_2 \in F_q[x] \ \ where$$
$$d_1 = \gcd(u_1, u_2), d_1 = e_1 u_1 + e_2 u_2$$

- Step2,Use the Euclidean algorithm to find polynomials

$$d, c_1, c_2 \in F_q \ \ where$$
$$d = \gcd(d_1, v_1 + v_2),$$
$$d = c_1 d_1 + c_2 (v_1 + v_2)$$

- Step3:

Let

$$s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2, so\ that$$
$$d = s_1 a_1 + s_2 a_2 + s_3 (b_1 + b_2)$$

- Step4

Set

$$a = a_1 a_2 / d^2$$

$$b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3 (b_1 b_2 + f)}{d} \mod a$$

$$if \quad \deg a \neq g + 1$$

$$b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3 (b_1 b_2 + f)}{d} \mod a \quad + a$$

$$if \quad \deg a = g + 1$$

- Reduction part

Step1:

Set

$$a' = (f - b^2)/a$$
$$b' = -b \mod a'$$

Step2:

If deg(a')>g then set a←a',b ←b' and go to step1.

Step3:

Let c be the leading coefficient of a',and set

$$a \leftarrow c^{-1}a'$$

- **例**:Genus 2**の場合**

$$D_1 = P_1 + P_2 + a_1 O + b_1 O' \text{ ,} \quad D_2 = Q + a_2 O + b_2 O'$$

この時はb**を従来どおりにとると、二つの有理点の和に同値な、有限点が三つの有理点が計算され、意味を成さなくなる。**

無限遠点の係数の調整

- これまでの計算で、求める被約因子の有限点の部分はわかった。

$D_1 + D_2$の通常点の数をd, D_3の通常点の数をd’とする。D_3 の無限遠点の部分の係数を求めることで加法は終了する。

Components at infinity

$$D_1 = [(u_1, v_1), a_1 O, b_1 O']$$

$$D_2 = [(u_2, v_2), a_2 O, b_2 O']$$

ならば

$$D_3 = [(u_3, v_3), a_1 + a_2 + \tfrac{d - d' - 1}{2}, b_1 + b_2 + \tfrac{d - d' + 1}{2}] \ \ if \ \ d + d' : odd$$

$$D_3 = [(u_3, v_3), a_1 + a_2 + \tfrac{d - d'}{2}, b_1 + b_2 + \tfrac{d - d'}{2}] \ \ if \ \ d + d' : even$$

example

$$y^2 = x^6 + 1 \ \ on \ \ Z/13Z$$

$$D_1 = [x(x-2), -7(x-2), -1, -1]$$

$$D_2 = [x-5, 0, 0, -1]$$

$$D_3 = [x^2 + 5x + 11, 2x + 2, -1, -1]$$

- $y^2 = x^6 + a_6, y^2 = x^6 + a_2 x^4 + a_6$ **という定義式の場合、**regulator**は**3**となる。よって、この場合の加法は**regulator**を求める作業を省略できる。**