３同種写像に付随するセルマー群の高速計算アルゴリズム

2013 年 1 月 26 日（土）髙妻倫太郎
立命館アジア太平洋大学
rintaro@apu.ac.jp

はじめに

代数体上の楕円曲線の階数の上限を与えるセルマー群は、その計算可能性が理論的に保障されている重要な数論的対象であり、現在、代数系処理ソフト Magma をはじめとした様々な数学ソフトウェアに計算アルゴリズムが実装されている。今回、有理数体上の位数３の有理点をもつ任意の楕円曲線に対して、論文（R.Kozuma, Rocky Mountain J. Math., Vol.40, No.4 (2010), 1227--1255.）の“公式”を応用したセルマー群の計算アルゴリズムを、コンソールアプリとして Visual C++2010 で実装した。この“公式”（図１）では、セルマー群の計算に必要となるガロアコホモロジーの局所連結準同型の像を、約４回の単純な条件分岐（数値の大小比較、剰余計算）のみで決定することが可能であり、既存のアルゴリズムを高速化すると期待される。

プログラムについて

本プログラムは、１つのソースファイル（main.cpp）および３つのヘッダファイル（ellcv.h、arith.h、prime.h）からなる。main.cpp（2 頁）ではコンソールのメインルーチンを実行し、ellcv.h（3 頁）では楕円曲線と悪還元をもつ素数に関する２つのクラス（EllCv、BadPrime）を定義した。また、prime.h では 49999 番目までの素数をテーブル化し、必要となる数論的関数を arith.h に記述した。全体的な処理の流れとしては、ユーザーからの係数（A・B）入力取得後、悪還元をもつ素数における小平記号および局所連結準同型の像を論文（R.Kozuma, 2010）の“公式”で決定・格納し、それを用いてセルマー群を計算・出力する。

開発環境

ＣＰＵ	Intel Core i5-2520M(モバイル) 2.50GHz
メモリ	4GB
ＯＳ	Windows 7 Professional (64bit)
開発	Visual Studio 2010 (C++)

～簡易フローチャート～

位数３の有理点をもつ $\mathbb{Q}$ 上の任意の楕円曲線

$$E : y^2 + Axy + By = x^3 \quad (A, B \in \mathbb{Z})$$

↓ A, B 入力

悪還元をもつ素数を計算

$$\Phi = \{\text{悪還元をもつ素数}\} \cup \{3\}$$

↓

局所連結準同型の像を計算

$$\hat{\delta}_p : E(\mathbb{Q}_p) \to \mathbb{Q}_p^*/\mathbb{Q}_p^{*3}$$

↓

セルマー群の計算

$$S^{(\hat{\phi})}(\widehat{E}/\mathbb{Q}) \simeq \left\{ d \in \mathbb{Q}^*/\mathbb{Q}^{*3} \;\middle|\; \begin{array}{c} d \in \mathrm{Im}\,\hat{\delta}_p \quad (^\forall \text{prime } p \in \Phi) \\ \nu_p(d) \equiv 0 \pmod 3 \quad (^\forall \text{prime } p \notin \Phi) \end{array} \right\}$$

↓

双対セルマー群の計算（カッセルズの公式）

$$\#S^{(\phi)}(E/\mathbb{Q}) = \#S^{(\hat{\phi})}(\widehat{E}/\mathbb{Q}) \times \frac{\#E(\mathbb{Q})[\phi]}{\#\widehat{E}(\mathbb{Q})[\hat{\phi}]} \prod_p \frac{\hat{c}_p}{c_p}$$

↓ 出力

セルマー群による上限

$$\mathrm{rank}E(\mathbb{Q}) \leq \dim_{\mathbb{F}_3} S^{(\hat{\phi})}(\widehat{E}/\mathbb{Q}) + \dim_{\mathbb{F}_3} S^{(\phi)}(E/\mathbb{Q}) - 1$$

実行ファイルダウンロードはこちら

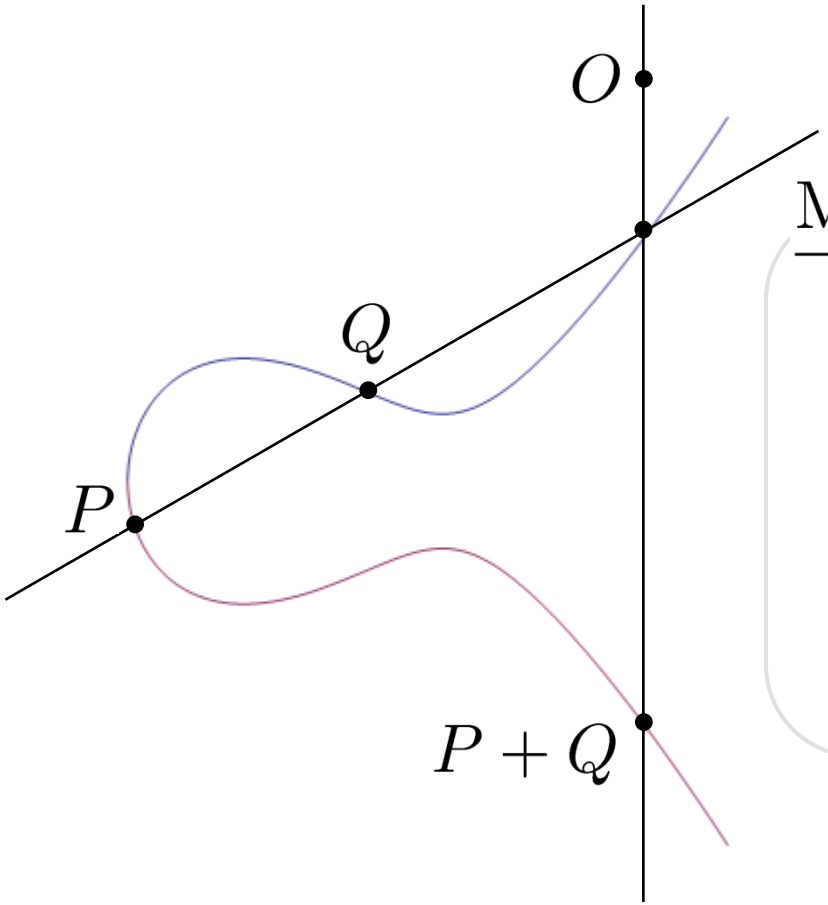
http://www.apu.ac.jp/~rintaro/program

３同種写像に付随するセルマー群の高速計算アルゴリズム

2013年1月26日（土）

髙妻倫太郎
立命館アジア太平洋大学

E : elliptic curve / a number field F $\ni$ a rational point O



Mordell-Weil Theorem (1922,-28)

$$E(F) \simeq \bigoplus_{i=1}^{t} \mathbb{Z}/d_i\mathbb{Z} \bigoplus \mathbb{Z}^r$$

$\mathrm{rank}E(F)$

Selmer groups give upper bounds for $\mathrm{rank}E(F)$
(effectively computed)

Set

- $F = \mathbb{Q}$
- $E/\mathbb{Q}$ has a rational 3-torsion point

$$E : y^2 + Axy + By = x^3 \quad (A,\, B \in \mathbb{Z})$$

Selmer groups $S^{(\phi)}(E/\mathbb{Q})$, $S^{(\hat{\phi})}(\widehat{E}/\mathbb{Q})$

$$\mathrm{rank}E(\mathbb{Q}) \leq \dim_{\mathbb{F}_3} S^{(\hat{\phi})}(\widehat{E}/\mathbb{Q}) + \dim_{\mathbb{F}_3} S^{(\phi)}(E/\mathbb{Q}) - 1$$

$\phi : E \to \hat{E}$: isogeny
$\hat{\phi} : \hat{E} \to E$: dual isogeny

Under our condition

$$\hat{\delta}_p : E(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p^* / \mathbb{Q}_p^{*3}$$

$$S^{(\hat{\phi})}(\widehat{E}/\mathbb{Q})$$

$$\simeq \left\{ d \in \mathbb{Q}^* / \mathbb{Q}^{*3} \;\middle|\; \begin{array}{c} d \in \operatorname{Im} \hat{\delta}_p \quad (^\forall \text{prime } p \in \Phi) \\ \nu_p(d) \equiv 0 \pmod 3 \quad (^\forall \text{prime } p \notin \Phi) \end{array} \right\}$$

$$\Phi = \{\text{bad primes for } E/\mathbb{Q}\} \cup \{3\} \text{ (finite)}$$

This Selmer group is a subgroup of the finite group

$$R = \left\{ d \in \mathbb{Q}^* / \mathbb{Q}^{*3} \;\middle|\; \nu_p(d) \equiv 0 \pmod 3 (^\forall \text{prime } p \notin \Phi) \right\}$$

Algorithm

step 1. Compute $S^{(\hat{\phi})}(\widehat{E}/\mathbb{Q})$ by searching all the elements in the finite group R contained in $\operatorname{Im}\hat{\delta}_p$ for every p

step 2. Compute (Cassels' formula)

$$\#S^{(\phi)}(E/\mathbb{Q}) = \#S^{(\hat{\phi})}(\widehat{E}/\mathbb{Q}) \times \frac{\#E(\mathbb{Q})[\phi]}{\#\widehat{E}(\mathbb{Q})[\hat{\phi}]} \prod_p \frac{\hat{c}_p}{c_p}$$

○ ⋯ use the 'formula' proven in

"R.Kozuma, Rocky Mountain J. Math., Vol.40, No.4 (2010), 1227–1255."