

# 代数体上の楕円曲線の計算に関する いくつかの話題\*

木田雅成<sup>†</sup>  
電気通信大学

## はじめに

有理数体上で定義された楕円曲線については、有理点をはじめとする様々な不変量の計算に関するアルゴリズムの研究は古くから行われており、多くの実装もあって、現在ではかなり満足できるレベルにあると言える。一方、有理数体よりも大きい体で定義された楕円曲線に関しては、対応する研究・実装は非常に少ないという状態が続いてきた。しかし、ここ数年でこの状況は少しずつ変わりつつある。この講演では有理点と reduction の二つの話題を取り上げ、現在の状況と、これからの課題を解説した。

## 1 Mordell-Weil 群について

$E$  を代数体  $K$  上で定義された楕円曲線とすると、次の良く知られた定理が成り立つ。

**定理 1.1 (Mordell-Weil の定理).**  $E$  上の  $K$  有理点のなす群  $E(K)$  は有限生成アーベル群である。したがって、

$$E(K) \simeq \mathbb{Z}^r \oplus \text{有限群}.$$

$E(K)$  のことを Mordell-Weil 群と呼ぶ。

この節の前半では、この群の計算する方法を紹介する。後半では  $K$  を拡大体に取り替えたときの、Mordell-Weil 群の変化を調べる。

---

\*講演の時のタイトルは“Computational aspects of the arithmetic theory of elliptic curves”でした。

<sup>†</sup>この研究は文部省科学研究費補助金奨励研究 (A)(No. 11740009) の援助を受けています。

## 1.1 代数体上の楕円曲線の Mordell-Weil 群の計算

ここでは、定義体が有理数体よりも大きい場合にも通用する計算方法を紹介する。有理数体上の楕円曲線の Mordell-Weil 群の計算については、効率の高める工夫などが多く知られている。たとえば [26] や [4] をみよ。

### 1.1.1 Torsion points

まず有限位数の部分群を計算する。次の本質的には良く知られた定理を使う。

**定理 1.2 ([15, Theorem 2.1]).**  $E$  の  $K$  上のモデルをひとつとっておく。  $\mathfrak{p}$  を  $p$  の上にある  $K$  の素イデアルで、  $\mathfrak{p} \nmid \Delta_E$  をみたすものとする。ここで、  $\Delta_E$  は上でとったモデルの判別式である。  $e = e(\mathfrak{p}, K/\mathbb{Q})$  を  $\mathfrak{p}$  の  $K/\mathbb{Q}$  での分岐指数とする。このとき  $\#(E(K)_{tors})$  は  $\#(\tilde{E}(O_K/\mathfrak{p})) \times p^{2t}$  の約数である。ただし、ここで

$$t = \begin{cases} 0 & p-1 > e \text{ のとき,} \\ \max\{r \in \mathbb{Z}_{>0} \mid (p-1)p^{r-1} \leq e\} & \text{それ以外.} \end{cases}$$

この定理を使うと次のようなアルゴリズムが考えられる。

**アルゴリズム 1.3 (cf. S. Schmitt [15]).**

**Step 1**  $\mathfrak{p} \nmid \Delta_E$  をみたすような小さな素イデアルをいくつか選ぶ。

**Step 2** Step 1 で求めた素イデアルに対して、定理 1.2 を使って、位数の上限を計算する。

**Step 3** 求めた上限の約数に対して、division polynomial を計算して実際の torsion point を求める。

このアルゴリズムを数論ソフト KASH [5] 上の楕円曲線計算ライブラリである TECC [13] に実装したものを次の例で示す。

**例 1.4.**

$$E/\mathbb{Q}(\sqrt{33}) : y^2 = x^3 - (162675 + 28296\sqrt{33})x + 35441118 + 6168312\sqrt{33}$$

この曲線は [14] の中にあるものである。

```
kash> ECTorsPts(E);
Primes used for bounding:[ 5, 7 ] # Step 1 の素数
Bound by 5: 18 # 定理 1.2 (p=5)
Bound by <7>: 54 # 定理 1.2 (p=7)
Bound for the torsion: 18
Actual torsion points found are # 見つかった torsion points
[ [ [ [114, 57], 0 ], 2 ], [ [ [171, 72], [1056, 480] ], 3 ],
  [ [ [171, 72], [-1056, -480] ], 3 ], [ [ [195, 48], [216, -216] ], 9 ],
  [ [ [195, 48], [-216, 216] ], 9 ], [ [ [267, 120], [5184, 2160] ], 9 ],
  [ [ [267, 120], [-5184, -2160] ], 9 ], [ [ [987, 408], [46224, 19440] ], 9 ],
  [ [ [987, 408], [-46224, -19440] ], 9 ] ]
[ 18, [ 18 ], [ [ [-237, -96], [-3672, -1512] ] ] ] # [群位数, 群構造, [生成元]]
Time: 880 ms
```

つまり  $E(\mathbb{Q}(\sqrt{33}))_{tors} \simeq \mathbb{Z}/18\mathbb{Z}$  で、その生成元は  $(-285 - 48\sqrt{33}, -4428 - 756\sqrt{33})$  であることがわかる<sup>1</sup>。この群は有理数体上では現れない。

このアルゴリズムでもっとも時間がかかるのは Step 3 である。もし Step 2 でよい限界がえられないと division polynomial の次数が非常に高くなり、計算に多くの時間がかかってしまう。有理数体や、二次体上のように、位数に explicit な上限が知られていれば、群構造を利用して、これをある程度軽減することはできる。

### 1.1.2 階数と基底の計算

次に Mordell-Weil 群の自由部分の計算に移る。この計算が一般の代数体で可能になったのはここ一、二年ほどのことである。その背景には、いろいろな不定方程式の計算解法が開発され、しかもそれが一般の整数環上で可能になったことがある。さらにさかのぼれば、Pari-GP[1] や KANT/KANT のような整数論ソフトの充実で、代数体の整数論の具体的な計算が手軽に計算機の上で実行可能になったということも無視できないであろう。

さて、この計算には、いろいろな variant が知られているが、以下ではもっとも一般的なものを示す。

計算の手順は次の二つに分かれる。

#### 2-descent 完全系列

$$1 \rightarrow E(K)/[2]E(K) \rightarrow S^{(2)}(E/K) \rightarrow \text{III}(E/K)[2] \rightarrow 1$$

を使って、 $E(K)/[2]E(K)$  の生成元を求める。

**Infinite descent**  $E(K)/[2]E(K)$  から  $E(K)$  を復元する。

これらの手順は本質的には以前から知られていたものである。したがって、ここでは、アルゴリズムの詳細な解説はせずに、その概略と代数体上の楕円曲線に適用するときの問題点を説明する。アルゴリズムの概要の読みやすい解説が [23, Chapter 7] にある。これを読んだあとに、より詳細な [4] や Simon の論文 [22] を読むとわかりやすい。

さて、2-descent を一般の代数体に適用する方法は [22] で与えられている。この論文で Simon が与えたのは Selmer 群  $S^{(2)}(E/K)$  を求める途中で現れる不定方程式をある種のノルム方程式に帰着する部分と、Selmer 群の元として現れる、ある 4 次不定方程式の係数を小さくする工夫の部分である。Simon の論文には 2 次体と 5 次体の楕円曲線について具体例が計算してある。

この Simon の方法で問題になるのが、定義体  $K$  の 3 次拡大のイデアル類群の構造と単数群の計算が必要ということである。したがって、楕円曲線の係数によっては  $K$  が 3 次体や 4 次体でも計算が困難な場合がありうる。

<sup>1</sup> 計算機の出力は標準基底で書いてある。

また、一般に Tate-Shafarevich 群  $\text{III}(E/K)[2]$  を計算するアルゴリズムは知られていないので、2-descent は本来の意味でのアルゴリズムになってはいないことに注意しなくてはならない。このことは、ある 4 次不定方程式がすべての素点について局所的に解けるとときに大域的に解を持つかを決定することと同値である。実際の計算では、ある程度の大きさの解の上限をきめて、その範囲で、4 次不定方程式の解を探索して満足することになる。したがって、実際にこのステップで求まることが保証されているのは  $E(K)/[2]E(K)$  の階数の上限だけである。

Infinite descent の方法は、次の二つの定理に基づく。

**定理 1.5** (cf. [4, Lemma 3.5.2]). 実数  $B$  を集合

$$T = \{P \in E(K) \mid \widehat{h}(P) \leq B\}$$

が  $E(K)/[2]E(K)$  の完全代表系を含むようにととる。このとき、 $T$  は  $E(K)$  を生成する。

**定理 1.6** (Silverman [20], Siksek [18]). 任意の  $P \in E(K)$  に対して、

$$h(P) - \widehat{h}(P) \geq B'$$

をみたす  $B'$  が存在する。

上の定理で、 $h$  は absolute logarithmic height を、 $\widehat{h}$  は canonical height をあらわす。

**アルゴリズム 1.7.**

**Step 1**  $E(K)/[2]E(K)$  の完全代表系から、定理 1.5 をみたす  $B$  を計算する。定理 1.6 を考えにいれると  $E(K)$  の生成元は  $h(P) \leq B + B'$  をみたす。

**Step 2**  $h(P) \leq B + B'$  なる  $P$  をすべて探し、群を大きくしていく。

一般の代数体上の楕円曲線に infinite descent を適用するときの問題点は Step 2 の計算に非常に時間がかかるということである。実際、 $P \in E(K)$  とし、

$$\text{Irred}(x(P), \mathbb{Z}; t) = a_0 t^n + \cdots + a_n = a_0 \prod_{j=1}^n (t - \alpha^{(j)}), \quad a_i \in \mathbb{Z}$$

とかくと、 $h(P) \leq B$  の点をすべて探すには、なにも工夫をしないと、

$$\max\{|a_0|, |a_1|, \dots, |a_n|\} \leq 2^{n-1} \exp(Bn)$$

の範囲の多項式をすべて探さねばならない ([19, VII, 5.9]). また、有理数体上の楕円曲線の時に有効であった、ふるいの方法が代数体の場合には直接は適用できない。

結果として、2-descent に比べて、infinite descent が非常に時間がかかるというのが現状である。

以上に解説したアルゴリズムの実装としては Simon の Pari/GP 上への実装<sup>2</sup>と Bruin の KASH への実装<sup>3</sup> (2-descent のみ) がある。

## 1.2 体の拡大

次の予想は有名である。

予想 1.8. 有理数体上定義された楕円曲線で rank がいくらかでも大きなものが存在する。

しかし、 $\mathbb{Q}$  上では rank の大きい曲線を作るのは、この報告集の長尾氏の解説にもあるように非常に難しい。

さて、 $E$  を代数体  $K$  上定義されている楕円曲線とすると、 $K$  の任意の有限次拡大体  $L$  に対して、Mordell-Weil 群  $E(L)$  を考えることができる。このように、体の拡大を許すと rank の大きな楕円曲線は比較的簡単に構成できる<sup>4</sup>。

例 1.9 (Kida [10]).  $E$  を  $y^2 = x^3 - x$  で与えられる  $\mathbb{Q}$  上の楕円曲線とする。

$$K_m = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_2}, \dots, \sqrt{q_m})$$

とおく。ただし、ここで、 $q_i$  は相異なる素数で mod 8 で 5 または 7 に合同なものとする。このとき、 $m$  を大きくすると、 $\text{rank}(E, K_m)$  はいくらでも大きくなる。

実際に rank の下限も与えることができる。

他方、同じ曲線について、次のような例も知られている。

例 1.10 (Iskra [6]).  $E$  は上の例と同じ  $y^2 = x^3 - x$  とする。

$$L_m = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_m})$$

とおく。ここで、 $p_i$  は相異なる素数で  $p_i \equiv 3 \pmod{8}$  かつ任意の  $j < i$  について、 $\left(\frac{p_j}{p_i}\right) = -1$  をみたすとする。このときすべての  $m$  について、 $\text{rank}(E, L_m) = 0$ 。

このほかに岩澤理論を使った例もいくつか知られている。

このような例は、体の数論が有理点の多寡に関わっているということを端的に示す簡単な例といえるであろう。

---

<sup>2</sup><http://www.math.u-bordeaux.fr/~desimon/maths/elliptic.html>. ただし筆者はまだプログラム自体を未入手である。

<sup>3</sup><http://msri.org/people/members/bruin/>

<sup>4</sup>このことは良く知られていると思っていたが、意外に知られていないことに最近気づいた。具体例もあまり知られていないようなので、この機会に紹介させていただいた。

## 2 Potential good reduction

楕円曲線の reduction を決定するアルゴリズムは「Tate のアルゴリズム」([21, IV,§9]) として, 以前から知られていた. しかし, 任意の代数体に通用する実装が登場したのは, 梅垣氏による Pari-GP への実装 [25] が (筆者の知る限り) 最初であり, その後, 筆者自身も KASH 上で実装を行った ([11]).

この節では, このプログラムを使って行われた, ある定理の発見の過程を述べてみたいと思う.

### 2.1 定義と定理

まず, この節で取り上げる potential good reduction という現象を例で説明する. 有理数体上の楕円曲線

$$E : y^2 + y = x^3 + x^2 - 8x + 19$$

を考える. この model の判別式は  $\Delta = -5^6 11$  であり, この方程式がいわゆる global minimal model を与えていることがわかる. 楕円曲線の global minimal model の判別式の素因数をみれば,  $E$  が  $p = 5$  と  $11$  以外では, 係数を  $\text{mod } p$  することによって, 有限体  $\mathbb{F}_p$  上の楕円曲線が得られることがわかる.  $E$  は  $p = 5, 11$  で bad reduction, それ以外の素点で good reduction をもつといわれるのであった.

さて, ここで取り上げるのは次の事実である.

Reduction は定義体によってかわる.

上の  $E$  について, このことをみしてみる.  $E$  を  $\mathbb{Q}(\sqrt{5})$  上の曲線とみると,  $5$  上の素点での判別式の付値の値は  $12$  になり minimal でなくなってしまう.

$[u, r, s, t]$  で楕円曲線の同型

$$\begin{cases} x = u^2 x' + r \\ y = u^3 y' + s u^2 x' + t \end{cases},$$

をあらわすことにすると,  $[-7 + \sqrt{5}, -2, 0, -13 + 5\sqrt{5}]$  によって, global minimal model

$$y^2 + y = x^3 - \frac{3 + \sqrt{5}}{2} x^2 + 2 + \sqrt{5}$$

をえる. この model の判別式を  $\Delta'$  とすると

$$\Delta' = -1771 - 792\sqrt{5}, (\Delta') = p_{11} p'_{11}$$

となる. ここで,  $p_{11}, p'_{11}$  は  $11$  の上の素イデアルである. したがって,  $E$  は  $\mathbb{Q}(\sqrt{5})$  上では  $5$  の上の素点で good reduction になる.

定義 2.1. このように有限次拡大をすると good reduction になるとき potential good reduction という.

いったん, ある素点で good reduction を持てば, 以降どのような拡大を作ってもその素点では good reduction のままであることが知られている ([19, VII, 5.4]).

次の定理も良く知られている.

定理 2.2 ([19, VII, 5.5]).  $E$  が  $p$  で potential good reduction であるための必要かつ十分な条件は  $v_p(j_E) \geq 0$  となることである.

とくに  $j_E$  が有理整数なら至るところで potential good reduction をもつ.

上の曲線  $E$  の  $j$  不変量は

$$j_E = -\frac{4096}{11}$$

である. したがって 5 の上の素イデアルでは potential good reduction を持つことが, これからもわかる. また, どのような拡大体を作っても 11 上の素点では good reduction にならないということもわかる.

さて, この状況の下で次のような問題を考えるのは自然であろう.

問題 2.3. 有理数体上の楕円曲線  $E$  が至るところで potential good reduction をもつとき,  $E_K$  がいたるところ good reduction になる  $K$  はどれだけ大きい, どれだけ小さいか. ここで  $E_K$  は  $E$  を  $K$  上の楕円曲線とみなしたもの (base change) をあらわす.

次の定理は上の問題への一つの解答を与えるものである.

定理 2.4 (Serre–Tate [16]).  $E$  を  $\mathbb{Q}$  上の楕円曲線として, あらゆる素点で potential good reduction を持つと仮定する. 3 以上の自然数  $m$  を  $E$  の bad prime と互いに素であるようにとる. このとき,  $E$  は  $m$  等分点の体  $\mathbb{Q}(E_m) = \mathbb{Q}(\{P \in E(\overline{\mathbb{Q}}) \mid mP = O\})$  上ではあらゆる素点で good reduction になる.

しかしながら, 等分点の体というのは一般に非常に大きいことが知られている. より小さい  $K$  はとれないのだろうか. 筆者は最近,  $K$  の次数に関する制限を与え次の二つの定理を証明することができた ([12]).

定理 2.5.  $E$  を  $\mathbb{Q}$  上定義された楕円曲線で  $j_E \in \mathbb{Z}$  をみたすものとする.  $\gcd([K : \mathbb{Q}], 6) = 1$  ならば  $E_K$  がすべての素点で good reduction になることはない.

定理 2.6.  $E$  を  $\mathbb{Q}$  上定義された楕円曲線で  $j_E \in \mathbb{Z}$  をみたすものとする.  $[K : \mathbb{Q}] = 2$  ならば  $E_K$  がすべての素点で good reduction になることはない.

したがって,  $K$  は一番小さい場合で 3 次体であることがわかる. 実際にそのような例をあとで与える (例 2.9).

ここでは, 定理 2.5 の証明をする過程において, どのように計算機が使われたかをみることを主眼にする<sup>5</sup>.

<sup>5</sup>定理 2.6 の証明は定理 2.5 の証明よりはるかに複雑である. 一言でいえば, quadratic twist と reduction の関係を細かく調べるということになる.

## 2.2 定理 2.5 の証明の発見

$E/\mathbb{Q}$  を  $\gcd([K:\mathbb{Q}], 6) = 1$  であるような体で、あらゆる素点で good reduction になるような楕円曲線とする.  $p$  を  $E$  の bad prime とする. このような  $p$  は必ず存在することが知られている.  $\Delta$  を  $E$  の  $p$ -minimal model の判別式とする.  $p$  上の  $K$  の素イデアル  $\mathfrak{p}$  をひとつとると,  $\mathfrak{p}$  で good reduction になることから,

$$v_p(\Delta)e(K/\mathbb{Q}, \mathfrak{p}) = v_p(\Delta) \equiv 0 \pmod{12}$$

とならなくてはならない. 次数に関する仮定から、特に  $e(K/\mathbb{Q}, \mathfrak{p})$  は 6 と素であるから、

$$(0 <) v_p(\Delta) \equiv 0 \pmod{12}.$$

したがって,  $p \geq 5$  なら  $p$ -minimal であることに反する. 以上より,  $p$  は 2 または 3 としてよい. つまり,  $E$  は 2 または 3 以外では good reduction をもち, 判別式の 2 または 3 での付値が 12 の倍数であるような  $\mathbb{Q}$  上の楕円曲線である. ところで Coghlan は博士論文で 2, 3 以外では bad reduction を持たない楕円曲線の決定をおこなっており, その結果が [2, Table 4] にのっている. そのなかで  $v_p(\Delta) \equiv 0 \pmod{12}$  ( $p = 2, 3$ ) をみたすのは,

$$E^\pm : y^2 = x^3 \pm 4x, \Delta = \pm 2^{12}, j = 1728$$

のふたつの曲線だけ. よって定理を証明するには次の主張が言えれば良い.

**主張 2.7.**  $E^\pm : y^2 = x^3 \pm 4x$  は  $\gcd([K:\mathbb{Q}], 6) = 1$  なる体  $K$  で good reduction にならない.

この主張をより証明しやすい明確なものにするために, TECC を使って, 実験を試みよう.  $K_n = \mathbb{Q}(\sqrt[n]{2})$ , ( $n = 1 \dots 20$ ) として,  $E_{K_n}^+$  の reduction を計算してみる.

```
E:=ECInit([0,0,0,4,0],Z);
for i in [2..20] do
  EM:=ECMove(E,OrderMaximal(Z,i,2));
  red:=ECGlobalReduction(EM);
  Print(i,"\t",red[2][1][2],"\n");
od;
```

という短い program で用は足りる. その結果は, 以下の表 1 の通り.

この表を良く見てみると, 奇数次の体で規則性がありそう. 実際に, 主張 2.7 の改良版として次の命題が成立する.

**命題 2.8.**

$$E^+ : y^2 = x^3 + 4x$$

は分岐指数  $e = e(\mathfrak{p}_2, K/\mathbb{Q})$  が奇数である体  $K$  で, 2 上の素イデアルにおける reduction type は  $\text{Type}(E^+, K) = I_{3e}^*$  となる. 特に奇数次の体では good reduction にならない.

Program Output		Kodaira Symbol	
degree	code		
2	-3	III*	
3	-13	I <sub>9</sub> *	←
4	-7	I <sub>3</sub> *	
5	-19	I <sub>15</sub> *	←
6	3	III	
7	-25	I <sub>21</sub> *	←
8	-3	III*	
9	-31	I <sub>27</sub> *	←
10	-3	III*	
11	-37	I <sub>33</sub> *	←
12	-13	I <sub>9</sub> *	
13	-43	I <sub>39</sub> *	←
14	3	III	
15	-49	I <sub>45</sub> *	←
16	-7	I <sub>3</sub> *	
17	-55	I <sub>51</sub> *	←
18	-3	III*	
19	-61	I <sub>57</sub> *	←
20	-19	I <sub>15</sub> *	

表 1: Reduction of  $E^+$  over  $\mathbb{Q}(\sqrt[n]{2})$

いったん, このように命題が明確に定式化されれば何とか証明はできるもので, 実際, この命題の証明は Tate のアルゴリズムを精密に適用することで得られる.  $E^-$  についても同様の命題が証明できて, 定理の証明も終わる.

良く知られているように, 楕円曲線の 2 または 3 上の reduction は, 計算するのも複雑であるし, その base change における振る舞いも簡単に記述できるようなものではないようである.

### 2.3 いくつかの例

先にのべたように  $\mathbb{Q}$  上の楕円曲線が base change であらゆる素点で good reduction をもつようになるには, 3 次体が最小の体になる.

例 2.9.

$$E : y^2 = x^3 + x^2 - 114x - 127, \Delta = 2^4 7^8.$$

この曲線は [4] の 196B1 である.  $K$  を  $f(X) = X^3 + 52X^2 + 444X + 7596$  で定義される 3 次体 とする. このとき  $E_K$  は, あらゆる素点で good reduction をもつ.

$E$  は位数 3 の点  $(16, 49)$  をもつので, 3 等分点の体は小さくなって, 実は  $f(X)$  の分解体で 6 次の体になる. その 3 次部分体が  $K$  である.

次に四次体での例をあげる.

例 2.10 (4 次体).

$$E' : y^2 = x^3 + 78x - 1352, \Delta = 2^8 \cdot 3^2 \cdot 13^2,$$

$$K = \mathbb{Q}\left(\sqrt[4]{78 + 15\sqrt{26}}\right) \supset k = \mathbb{Q}(\sqrt{26}) \supset \mathbb{Q}$$

とすると,  $E'_K$  はあらゆる素点で good reduction をもつ. 一方,  $E'_k$  はそうではない.

この例から, 定理 2.6 の基礎体  $\mathbb{Q}$  を一般には取り替えることができないことがわかる.

$E'_k$  の  $K/k$  に対応する quadratic twist は  $k$  上の楕円曲線になるが, この曲線があらゆる素点で good reduction を持つことを示すことができる.

しかしながら, この現象はいつでもおこりうるというものではない. [4] の 49A2

$$E'' : y^2 + xy = x^3 - x^2 - 37x - 78$$

を考える.  $K = \mathbb{Q}(\sqrt[4]{-7}) \supset k = \mathbb{Q}(\sqrt{-7})$  とすると,  $E'_K$  はあらゆる素点で good reduction であるが,  $E'_k$  の  $K/k$  に関する twist は 2 上の素イデアルで  $I_4^*$  type の bad reduction をもつ<sup>6</sup>. これは 7 上の素イデアル以外に分岐がないような  $k$  上の 2 次拡大が存在しないことに由来するものである.

これらの例の計算にも TECC [13] を使った.

## Modular 多項式のデータの公開のお知らせ

Modular 多項式は modular curve  $X_0(n)$  の canonical model を与える方程式で,  $n$  が素数  $p$  のときは,

$$\Phi_p(X, j) = (X - j(pz)) \prod_{k=0}^{p-1} \left( X - j\left(\frac{z+k}{p}\right) \right)$$

によって与えられる. ここで,

$$j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \dots, q = \exp(2\pi\sqrt{-1}z).$$

富士通研究所が  $p \leq 113$  の Modular 多項式のデータを

<http://www.fujitsu.co.jp/hypertext/flab/modularpoly/index.html>

で公開中である<sup>7</sup>. それを補完する合成数の場合のデータを [7] の方法により,  $n \leq 50$  で生成したので, そのデータと, それらを Maple 上から使う program を生成する Perl で書かれた meta program を

<sup>6</sup>実は  $k = \mathbb{Q}(\sqrt{-7})$  上にはあらゆる素点で good reduction を持つ楕円曲線がないことが知られている ([17] と [24] をみよ).

<sup>7</sup>その計算方法については [8] と [9] を参照せよ.

<http://matha.e-one.uec.ac.jp/~kida/modularpoly.html>

で公開する. これを使うとたとえば Maple 上で次のような計算が可能になる.

```
> read modularpoly:
> modularpoly(4)(X,Y);

2976Y5X3 + 7440Y4X4 - Y4X5 - 94266583063223403127324218750000 YX
+ 188656639464998455284287109375 Y2X
- 22805180351548032195000000000 Y3
+ 188656639464998455284287109375 YX2
+ 26402314839969410496000000 Y2X2 + 1194227244109980000 YX4
- 914362550706103200000 Y2X3 + 2976 Y3X5
+ 12519806366846423598750000 Y3X - 914362550706103200000 Y3X2
+ 561444609 Y5X - 2533680 Y2X5 + 80967606480 Y4X3 + 80967606480 Y3X4
- 22805180351548032195000000000 X3
- 36493632779675765840437500000000000 X
- 36493632779675765840437500000000000 Y
+ 28094937472219537210964062500000000000 - 2533680 Y5X2
+ 561444609 YX5 + 1425220456750080 Y4X2 + 1425220456750080 Y2X4
+ 2729942049541120 Y3X3 + Y6 + 158010236947953767724187500000000 Y2
+ 158010236947953767724187500000000 X2 + X6 - 8507430000 X5
+ 24125474716854750000 Y4 + 24125474716854750000 X4 - 8507430000 Y5
- Y5X4 + 12519806366846423598750000 YX3 + 1194227244109980000 Y4X
> modularpoly(4)(X,Y)-modularpoly(4)(Y,X);

0
> factor(modularpoly(8)(X,X));

-(12167000000 - 52250000X + X2)(X + 3375)2(X - 16581375)2(X - 287496)2
(X3 + 3491750X2 - 5151296875X + 12771880859375)2
(X3 + 39491307X2 - 58682638134X + 1566028350940383)2
```

最後の因数分解には Hilbert class polynomial が出てくるわけである (cf. [3, Theorem 13.4]).

## 参考文献

- [1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and Olivier, *User's guide to PARI-GP version 2.0.17*, Laboratoire A2X, U.M.R. 9936 du C.N.R.S., Université Bordeaux I, June 1999.

<http://www.parigp-home.de/>. 1.1.2

- [2] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Springer-Verlag, Berlin, 1975, Lecture Notes in Mathematics, Vol. 476. 2.2
- [3] D. A. Cox, *Primes of the form  $x^2 + ny^2$* , John Wiley & Sons Inc., New York, 1989. 7
- [4] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. 1.1, 1.1.2, 1.5, 2.9, 2.10
- [5] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger, *KANT V4*, J. Symbolic Comput. **24** (1997), no. 3-4, 267–283, Computational algebra and number theory (London, 1993). 1.1.1
- [6] B. Iskra, *Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8*, Proc. Japan Acad. Ser. A Math. Sci. **72** (1996), no. 7, 168–169. 1.10
- [7] H. Ito, *Computation of modular equation. II*, Mem. College Ed. Akita Univ. Natur. Sci. (1997), no. 52, 1–10. 7
- [8] 伊豆哲也, Risa/Asir による modular polynomial の計算, 数理解析研究所講究録 (1998), no. 1038, 244–254, 数式処理における理論と応用の研究 (京都, 1997). 7
- [9] 伊豆哲也, 野呂正行, 横山和弘, モジュラー多項式の計算, 暗号と情報セキュリティシンポジウム (SCIS '98) 報告集, 1998. 7
- [10] M. Kida, *On the rank of an elliptic curve in elementary 2-extensions*, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), no. 10, 422–425. 1.9
- [11] 木田雅成, KASH による楕円曲線の計算, 第三回「代数学と計算」研究集会報告集, 東京都立大学, 1999.  
[ftp://tnt.math.metro-u.ac.jp/pub/ac99/kida/](http://tnt.math.metro-u.ac.jp/pub/ac99/kida/). 2
- [12] M. Kida, *Potential good reduction of elliptic curves*, (2000), Preprint. 2.1
- [13] ———, *TECC manual version 2.3*, The University of Electro-Communications, March 2000.  
<http://matha.e-one.uec.ac.jp/~kida/TECC.html>. 1.1.1, 2.3
- [14] M. A. Reichert, *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*, Math. Comp. **46** (1986), no. 174, 637–658. 1.4
- [15] S. Schmitt, *Determination of the Mordell-Weil group of elliptic curves over number fields*, Preprint (2000). 1.2, 1.3

- [16] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. 2.4
- [17] B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific J. Math. **74** (1978), no. 1, 235–250. 6
- [18] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain J. Math. **25** (1995), no. 4, 1501–1538. 1.6
- [19] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986. 1.1.2, 2.1, 2.2
- [20] ———, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), no. 192, 723–743. 1.6
- [21] ———, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994. 2
- [22] D. Simon, *Computing the rank of elliptic curves over number fields*, Preprint (2000).  
<http://www.math.u-bordeaux.fr/~desimon/math/elliptic.html>. 1.1.2, 1.1.2
- [23] N. P. Smart, *The algorithmic resolution of Diophantine equations*, Cambridge University Press, Cambridge, 1998. 1.1.2
- [24] R. J. Stroeker, *Reduction of elliptic curves over imaginary quadratic number fields*, Pacific J. Math. **108** (1983), no. 2, 451–463. 6
- [25] 梅垣敦紀, 代数体上の楕円曲線の計算, 第二回「代数学と計算」研究集会報告集, 東京都立大学, 1997.  
<ftp://tnt.math.metro-u.ac.jp/pub/ac97/PROCEEDINGS/umegaki/>. 2
- [26] H. G. Zimmer, *Basic algorithms for elliptic curves*, Number theory (Eger, 1996), de Gruyter, Berlin, 1998, pp. 541–595. 1.1

きだまさなり

〒182-8585 調布市調布が丘 1-5-1

電気通信大学 数学教室

e-mail: [kida@sugaku.e-one.uec.ac.jp](mailto:kida@sugaku.e-one.uec.ac.jp)

(講演 2000 年 8 月 31 日)

(提出 2000 年 11 月 22 日)