楕円曲線について

上越教育大学　　中川仁

平成10年9月17日

目 次

記号.　$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ によって，それぞれ整数全体の集合，有理数全体の集合，実数全体の集合を表す．整数 a, b の最大公約数を $\gcd(a, b)$ で表す．$\gcd(a, b) = 1$ のとき，a と b は互いに素であるという．整数 a, b の差が自然数 n で割り切れるとき，$a \equiv b \pmod{n}$ とかき，a と b は n を法として合同であるという．

0　はじめに

a, b を $4a^3 - 27b^2 \neq 0$ を満たす実数とする．そのとき，方程式

$$y^2 = x^3 - ax - b \tag{0.1}$$

によって定義される曲線 E を**楕円曲線**という．こう呼ばれる理由は，楕円の孤の長さを表す積分と関係があるためである．本講演では，楕円曲線 E 上に加法群の構造が入ること，a, b が有理数のとき，x, y ともに有理数であるような E 上の点の集合 $E(\mathbb{Q})$ が部分群をなすことを説明する．

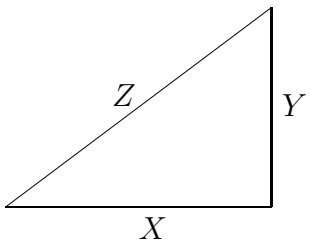
楕円曲線の整数論は，今世紀のはじめに Mordell によって「群 $E(\mathbb{Q})$ が有限生成である」という定理が証明されて以来，多くの整数論研究者の関心を集め，最も盛んに研究されている対象の一つである．Wiles による Fermat 予想の解決も，楕円曲線に関する谷山–志村の予想を解くことによって得られた．楕円曲線に関しては，多くの結果が知られているが，合同数の問題，BSD 予想等，多くの問題が未解決のまま残されている．また応用面でも，楕円曲線の加法を利用して大きな数を素因数分解する楕円曲線法が，暗号理論において注目されている．

1　ピタゴラス数

3 辺の長さが X, Y, Z の直角三角形は

$$X^2 + Y^2 = Z^2 \tag{1.1}$$

を満たす．等式 (1.1) を満たす自然数 X, Y, Z を**ピタゴラス数**と呼ぶ．



7 世紀頃，インドの Brahmagupta はピタゴラス数をすべて決定した．この問題は，$x = \dfrac{X}{Z}, y = \dfrac{Y}{Z}$ とおくことによって，単位円

$$C : x^2 + y^2 = 1 \tag{1.2}$$

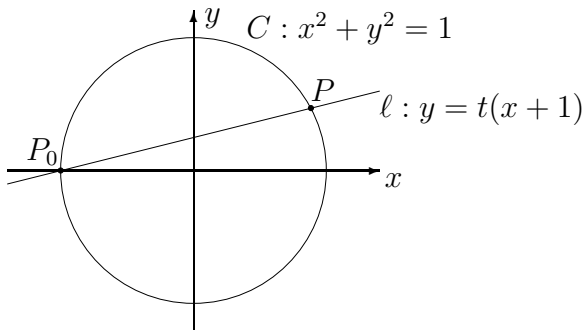


図 1: 円のパラメータ表示

上の**有理点** (x, y ともに有理数であるような点) を決定するという問題と同じになる．これは次のようにして解ける:

点 $P_0 = (-1, 0)$ を通る傾き t の直線 ℓ と単位円 C は P_0 以外にもう 1 点 P で交わる (図 1)．直線 ℓ の方程式 $y = t(x + 1)$ を (1.2) に代入して,

$$x^2 + t^2(x + 1)^2 = 1,$$

$$(1 + t^2)x^2 + 2t^2x + t^2 - 1 = 0,$$

$$(x + 1)\big((1 + t^2)x + t^2 - 1\big) = 0.$$

これから，点 P の座標は,

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2} \tag{1.3}$$

とパラメータ表示される．ここで，$t \in \mathbb{Q}$ ならば，$x, y \in \mathbb{Q}$ である．逆に $x, y \in \mathbb{Q}$ ならば，$t = \frac{y}{x+1} \in \mathbb{Q}$ である．以上によって，単位円 C 上の P_0 以外の有理点は，ある $t \in \mathbb{Q}$ によって，等式 (1.3) で表される．$t \in \mathbb{Q}$ を $t = \frac{b}{a}$, $a, b \in \mathbb{Z}$，$a > 0$，$\gcd(a, b) = 1$ とかく．そのとき,

$$x = \frac{a^2 - b^2}{a^2 + b^2}, \quad y = \frac{2ab}{a^2 + b^2}$$

である．$\gcd(a, b) = 1$ であるから，素数 p が $2ab$ と $a^2 + b^2$ をともに割り切ったとすると，$p = 2$ でなければならない．そのとき，a, b はともに奇数であるから，$a = 2a_1 + 1$, $b = 2b_1 + 1$ とおくと,

$$x = \frac{2(a_1 - b_1)(a_1 + b_1 + 1)}{2a_1^2 + 2a_1 + 2b_1^2 + 2b_1 + 1}, \quad y = \frac{(2a_1 + 1)(2b_1 + 1)}{2a_1^2 + 2a_1 + 2b_1^2 + 2b_1 + 1}.$$

ここで，$A = a_1 + b_1 + 1$, $B = a_1 - b_1$ とおけば，

$$x = \frac{2AB}{A^2 + B^2}, \quad y = \frac{A^2 - B^2}{A^2 + B^2}$$

であり，$A^2 + B^2$ は奇数であるから，$\frac{2AB}{A^2+B^2}$, $\frac{A^2-B^2}{A^2+B^2}$ はともに既約分数である．また，A, B の一方だけが奇数である．はじめから，$2ab$ と $a^2 + b^2$ が互いに素ならば，a, b の一方だけが奇数である．そのとき，$\frac{2ab}{a^2+b^2}$, $\frac{a^2-b^2}{a^2+b^2}$ はともに既約分数である．以上まとめると，

定理 1.1. 不定方程式

$$X^2 + Y^2 = Z^2$$

の自然数解 X, Y, Z で，X, Y, Z が互いに素であるものは，$a \not\equiv b \pmod 2$, $\gcd(a, b) = 1$ を満たす自然数 $a > b$ によって，

$$X = a^2 - b^2,\ Y = 2ab,\ Z = a^2 + b^2$$

または，

$$X = 2ab,\ Y = a^2 - b^2,\ Z = a^2 + b^2$$

と表せる．

この定理の応用として，不定方程式

$$X^4 - Y^4 = Z^2 \tag{1.4}$$

は自然数解を持たないことを証明しよう．(1.4) が自然数解 X, Y, Z を持ったとする．さらに，自然数解の中で X が最小になるものをとったとしてよい．そのとき，X, Y, Z は互いに素である．$(Y^2)^2 + Z^2 = (X^2)^2$ とみれば，定理 1.1 より，互いに素な自然数 $A > B$ で，$A \not\equiv B \pmod 2$ が存在して，

$$Y^2 = A^2 - B^2,\ Z = 2AB,\ X^2 = A^2 + B^2$$

または，

$$Z = A^2 - B^2,\ Y^2 = 2AB,\ X^2 = A^2 + B^2$$

と表せる．前者の場合，X, Y は奇数，Z は偶数である．よって，

$$X^4 - Y^4 = (X^2 + Y^2)(X^2 - Y^2) = Z^2$$

において，$X^2 + Y^2$ と $X^2 - Y^2$ はともに偶数である．$\gcd(X, Y) = 1$ であるから，$X^2 + Y^2$ と $X^2 - Y^2$ の最大公約数は 2 であることがわかる．

$Z = 2Z_1$, $X^2+Y^2 = 2U$, $X^2-Y^2 = 2V$, Z_1, U, V は自然数, $\gcd(U,V) = 1$ とかけば, $UV = Z_1^2$ より, $U = X_1^2$, $V = Y_1^2$ とかける. そのとき,

$$X_1^4 - Y_1^4 = U^2 - V^2 = (U+V)(U-V) = (XY)^2$$

である. $Y < X$ であるから,

$$X_1^2 = U = \frac{X^2+Y^2}{2} < X^2, \quad X_1 < X$$

である. これは X, Y, Z が (1.4) の自然数解の中で X が最小であるようにとったことに矛盾する.

後者の場合は, $Y^2 = 2AB$, $\gcd(A,B) = 1$ であることから, U, V を互いに素な自然数として, $A = U^2$, $B = 2V^2$ または $A = 2V^2$, $B = U^2$ とかける. これを $X^2 = A^2 + B^2$ に代入して,

$$X^2 = U^4 + 4V^4 = (U^2)^2 + (2V^2)^2$$

を得る. 再び定理 1.1 を適用すれば, 互いに素な自然数 a, b が存在して,

$$U^2 = a^2 - b^2, \quad 2V^2 = 2ab, \quad X = a^2 + b^2$$

である. $V^2 = ab$, $\gcd(a,b) = 1$ であるから, 自然数 X_1, Y_1 によって, $a = X_1^2$, $b = Y_1^2$ とかける. そのとき,

$$X_1^4 - Y_1^4 = a^2 - b^2 = U^2$$

である.

$$X_1 \le X_1^2 = a \le a^2 < a^2 + b^2 = X$$

であるから, これも X, Y, Z が (1.4) の自然数解の中で X が最小であるようにとったことに矛盾する.

以上まとめて, 次の定理を得る:

定理 1.2. 不定方程式

$$X^4 - Y^4 = Z^2$$

は自然数解を持たない. したがって, 不定方程式

$$X^4 + Y^4 = Z^4$$

も自然数解を持たない.

2　楕円曲線上の加法

a, b を $4a^3 - 27b^2 \neq 0$ を満たす実数として，楕円曲線

$$E : y^2 = x^3 - ax - b$$

を考える．$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ を E 上の異なる 2 点とする．そのとき，P_1 と P_2 を結ぶ直線 ℓ の方程式を

$$y = \lambda x + \mu$$

とする． ここで,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \mu = y_1 - \lambda x_1 = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}$$

である．曲線 E と直線 ℓ との交点は P_1 と P_2 以外にもう 1 点ある．それを $P_3 = (x_3, y_3)$ とする．そのとき，x_1, x_2, x_3 は 3 次方程式

$$x^3 - ax - b = (\lambda x + \mu)^2,$$

$$x^3 - \lambda^2 x^2 - (a + 2\lambda\mu)x - b - \mu^2 = 0$$

の根である．よって，根と係数の関係から,

$$x_1 + x_2 + x_3 = \lambda^2 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2,$$

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \tag{2.1}$$

である．また,

$$y_3 = \frac{y_2 - y_1}{x_2 - x_1} x_3 + \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1} \tag{2.2}$$

である．x_3, y_3 を等式 (2.1), (2.2) によって決めたとき，2 点 P_1 と P_2 の和 $P_1 + P_2$ を

$$P_1 + P_2 = (x_3, -y_3) \tag{2.3}$$

によって定義する (図 2).

$P_1 = P_2$ のときは，直線 ℓ を点 P_1 における曲線 E の接線とすれば, $y_1 \neq 0$ ならば，ℓ の方程式は

$$y = \lambda x + \mu$$

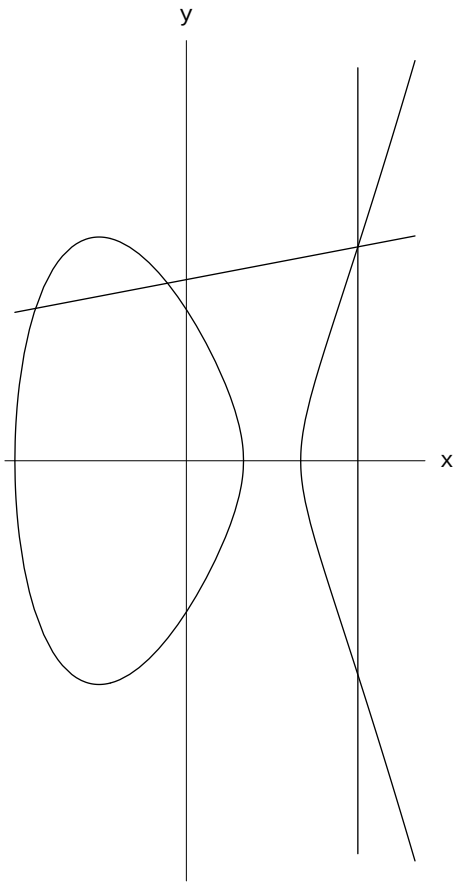


図 2: 楕円曲線上の加法

である．ここで，

$$2y\frac{dy}{dx} = 3x^2 - a$$

であるから，

$$\lambda = \frac{3x_1^2 - a}{2y_1}, \quad \mu = y_1 - \lambda x_1.$$

曲線 E と直線 ℓ との交点は接点 P_1 以外にもう 1 点ある．それを $P_3 = (x_3, y_3)$ とする．そのとき，x_1, x_3 は 3 次方程式

$$x^3 - ax - b = (\lambda x + \mu)^2,$$

$$x^3 - \lambda^2 x^2 - (a + 2\lambda\mu)x - b - \mu^2 = 0$$

の根であり，x_1 は重根である．よって，根と係数の関係から，

$$2x_1 + x_3 = \lambda^2 = \left(\frac{3x_1^2 - a}{2y_1}\right)^2,$$

$$x_3 = \left(\frac{3x_1^2 - a}{2y_1}\right)^2 - 2x_1 \tag{2.4}$$

である．また，

$$y_3 = \frac{3x_1^2 - a}{2y_1}(x_3 - x_1) + y_1 \tag{2.5}$$

である．x_3, y_3 を等式 (2.4), (2.5) によって決めたとき，2 点 P_1 の 2 倍 $2P_1$ を

$$2P_1 = (x_3, -y_3) \tag{2.6}$$

によって定義する．最後に，$P_1 = P_2$ かつ $y_1 = 0$ のとき，

$$2P_1 = P_\infty \quad (P_\infty \text{ は無限遠点})$$

とする．

このように加法を定義することによって，曲線 E は P_∞ を単位元とするアーベル群になることが示される．特に，a, b が有理数のとき，P_1, P_2 の座標が有理数ならば，$P_3 = P_1 + P_2$ の座標も有理数になることがわかる．したがって，E 上の有理点全体の集合 $E(\mathbb{Q})$ は E の部分群になることがわかる．

3 Mordellの定理

Mordellは1922年に次の定理を証明した.

定理 3.1 (Mordellの定理). $E(\mathbb{Q})$ は有限生成アーベル群である．すなわち，有限個の点 $P_1, \ldots, P_l \in E(\mathbb{Q})$ が存在して，任意の $P \in E(\mathbb{Q})$ は

$$P = n_1 P_1 + \cdots + n_l P_l, \quad n_i \in \mathbb{Z}$$

と表せる．したがって，T を有限アーベル群, $r \geq 0$ として,

$$E(\mathbb{Q}) \cong T \times \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{r}$$

である.

上の定理の r を $E(\mathbb{Q})$ の**ランク**という．$r > 0$ であることと $E(\mathbb{Q})$ が無限群であることは同値である.

有限位数の部分 T は次の定理によって，比較的容易に決定される.

定理 3.2 (Nagell–Lutzの定理). $a, b \in \mathbb{Z}$, $D = 4a^3 - 27b^2 \neq 0$ とする．$P = (x, y)$ を $E(\mathbb{Q})$ の有限位数の点とすれば，$x, y \in \mathbb{Z}$ であり，$y = 0$ であるかまたは y は D の約数である.

$r = 0$ となる具体例と $r > 0$ となる具体例をそれぞれ挙げてみよう.

例 3.3. $E : y^2 = x^3 - x$ とする.

$$P_\infty,\ (0,0),\ (1,0),\ (-1,0)$$

の4点は $E(\mathbb{Q})$ の元である．これら以外の $E(\mathbb{Q})$ の元は存在しないことを示そう．これらの点と異なる $E(\mathbb{Q})$ の元 (x, y) があったとすると，$y \neq 0$ である．$x = \frac{u}{v}$, $u, v \in \mathbb{Z}$, $\gcd(u, v) = 1$，$v > 0$ とかく．同様に，$y = \frac{s}{t}$, $s, t \in \mathbb{Z}$, $\gcd(s, t) = 1$，$t > 0$ とかく．そのとき,

$$\frac{s^2}{t^2} = \frac{u(u^2 - v^2)}{v^3}$$

であるが，両辺ともに既約分数であるから,

$$s^2 = u(u^2 - v^2), \quad t^2 = v^3$$

を得る．$t^2 = v^3$ の両辺の素因数分解を考えれば，$v = V^2$, $t = V^3$, $V \in \mathbb{Z}$ である．u と $u^2 - v^2$ は互いに素である．$s^2 = u(u^2 - v^2)$ の両辺の素因数分解を考えれば，u も $u^2 - v^2$ もともに平方数であるから，$u = U^2$, $u^2 - v^2 = W^2$, $U, W \in \mathbb{Z}$ とかける．よって，

$$U^4 - V^4 = W^2$$

である．しかし，これは定理 *1.2* によって，自然数解を持たない．ゆえに，

$$E(\mathbb{Q}) = \{P_\infty, (0,0), (1,0), (-1,0)\}$$

であり，ランクは 0 である．

例 3.4. $E : y^2 = x^3 - 5x$ とする．$P_1 = \left(\frac{9}{4}, \frac{3}{8}\right)$ は $E(\mathbb{Q})$ の元である．定理 *3.2* によって，P_1 は無限位数である．したがって，ランク r は 1 以上である．実は $r = 1$ である．$2P_1, 3P_1$ を計算すれば，

$$2P_1 = \left(\frac{25921}{144}, \frac{-4172959}{1728}\right),\ 3P_1 = \left(\frac{6197310729}{2620825636}, \frac{158681535363837}{134170547609384}\right)$$

である．

4　合同ゼータ関数

$a, b \in \mathbb{Z}$, $D = 4a^3 - 27b^2 \neq 0$ として，楕円曲線 $E : y^2 = x^3 - ax - b$ を考える．各素数 p に対して，合同式

$$y^2 \equiv x^3 - ax - b \pmod{p}$$

の解の個数を N_p とする．

$$a_p = p - N_p$$

とおく．そのとき，変数 t の有理関数

$$Z_{E,p}(t) = \frac{1 - a_p t + pt^2}{(1-t)(1-pt)}$$

を $E \bmod p$ の**合同ゼータ関数**という．

例 4.1. $E : y^2 = x^3 + x$ とする．$p = 3$ について，

$$0^3 + 0 = 0,\ 1^3 + 1 = 2,\ 2^3 + 2 = 10 \equiv 1 \pmod 3$$

であり，

$$y^2 \equiv 0 \pmod 3 \Longleftrightarrow y \equiv 0 \pmod 3,$$
$$y^2 \equiv 1 \pmod 3 \Longleftrightarrow y \equiv 1, 2 \pmod 3$$

であり，合同式 $y^2 \equiv 2 \pmod 3$ は解を持たない．したがって，$N_3 = 3$, $a_3 = 0$ であり，

$$Z_{E,3}(t) = \frac{1 + 3t^2}{(1 - t)(1 - 3t)}$$

である．$p = 5$ について，

$$0^3 + 0 = 0,\ 1^3 + 1 = 2,\ 2^3 + 2 \equiv 0,\ 3^3 + 3 \equiv 0,\ 4^3 + 4 \equiv 3 \pmod 5$$

であり，

$$y^2 \equiv 0 \pmod 5 \Longleftrightarrow y \equiv 0 \pmod 5,$$

であり，合同式 $y^2 \equiv 2 \pmod 5$ および $y^2 \equiv 3 \pmod 5$ はいずれも解を持たない．したがって，$N_5 = 3$, $a_5 = 2$ であり，

$$Z_{E,5}(t) = \frac{1 - 2t + 5t^2}{(1 - t)(1 - 5t)}$$

である．

Artin によって予想された次の不等式は，Hasse によって最初に証明された後に，Weil によって，一般の代数曲線に関する不等式として拡張された．

定理 4.2 (Hasse の定理). $|a_p| \leq 2\sqrt{p}$ が成り立つ．したがって，$Z_{E,p}(t)$ の分子の多項式は

$$1 - a_p t + pt^2 = (1 - \omega t)(1 - \overline{\omega} t)$$

と因数分解される．ここで，ω は絶対値 $\sqrt{p}$ の複素数である．

5　BSD 予想

s を複素変数とし，t に p^{-s} を代入して，すべての素数 p についての $Z_{E,p}(p^{-s})$ の分子の逆数の積をとって，

$$L_E(s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

を作る．$L_E(s)$ を E の **Hasse–Weil ゼータ関数**という．1963 年に，Birch と Swinnerton-Dyer は $E(\mathbb{Q})$ のランク r と $L_E(s)$ の $s = 1$ における零点の位数について，次の予想を提出した:

予想 5.1 (BSD 予想). r を $E(\mathbb{Q})$ のランクとすれば，*Hasse–Weil* ゼータ関数 $L_E(s)$ は全複素平面に解析接続され，$s = 1$ において，位数 r の零点を持つ.

この予想は多くの数学者によって研究されているが，現在でも部分的な結果しか得られていない．最初に得られた著しい結果は Coates と Wiles によって 1977 年に得られた次の定理である:

定理 5.2 (Coates–Wiles の定理). E を $\mathbb{Q}$ 上定義された虚数乗法を持つ楕円曲線とし，$E(\mathbb{Q})$ のランクを r とする．そのとき，$r > 0$ ならば $L_E(s)$ は $s = 1$ で零点を持つ.

6　合同数問題

自然数 n に対して，3 辺の長さが有理数であるような直角三角形で面積が n のものが存在するとき，n は**合同数**であるという.

例 6.1. 6 は合同数である．実際,

$$3^2 + 4^2 = 5^2, \quad \frac{1}{2} \times 3 \times 4 = 6.$$

5 が合同数であることはフィボナッチが示した (1225 年)．実際,

$$9^2 + 40^2 = 41^2$$

の両辺を 6^2 で割って,

$$\left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \left(\frac{41}{6}\right)^2, \quad \frac{1}{2} \times \frac{3}{2} \times \frac{20}{3} = 5.$$

n は合同数であるとする．すなわち，有理数 $X < Y < Z$ で，

$$X^2 + Y^2 = Z^2, \quad \frac{1}{2}XY = n$$

を満たすものが存在するとする．そのとき，

$$x = \frac{Z^2}{4}, \quad y = \frac{(Y^2 - X^2)Z}{8}$$

とおけば，

$$\begin{aligned} x^3 - n^2x &= x(x-n)(x+n) = \frac{Z^2}{4}\left(\frac{Z^2}{4} - n\right)\left(\frac{Z^2}{4} + n\right) \\ &= \frac{Z^2}{4}\left(\frac{X^2+Y^2}{4} - \frac{XY}{2}\right)\left(\frac{X^2+Y^2}{4} + \frac{XY}{2}\right) \\ &= \frac{Z^2}{4}\frac{(Y-X)^2}{4}\frac{(Y+X)^2}{4} \\ &= \left(\frac{Z(Y-X)(Y+X)}{8}\right)^2 = y^2. \end{aligned}$$

したがって，楕円曲線 $E_n : y^2 = x^3 - n^2x$ は有理点

$$P = \left(\frac{Z^2}{4}, \frac{(Y^2 - X^2)Z}{8}\right)$$

を持つ．$E_n(\mathbb{Q})$ の有限位数の点は

$$P_\infty,\ (0,0),\ (n,0),\ (-n,0)$$

の 4 点しかないことが示され，したがって，P は無限位数の点であることがわかり，$E_n(\mathbb{Q})$ のランクは $r > 0$ であることがわかる．逆に，$r > 0$ ならば，n は合同数であることも示される．以上によって，

命題 6.2. 自然数 n に対して，方程式 $y^2 = x^3 - n^2x$ で定義される楕円曲線を E_n とし，$E_n(\mathbb{Q})$ のランクを r とする．そのとき，n が合同数であるための必要十分条件は $r > 0$ である．

例 6.3. 楕円曲線 $E_1 : y^2 = x^3 - x$ について，$E_1(\mathbb{Q})$ のランクは例 3.3 によって 0 であったから，上の命題から 1 は合同数でないことがわかる．

E_n についての BSD 予想が正しいとすれば，n が合同数であることと E_n の Hasse–Weil ゼータ関数 $L_{E_n}(s)$ が $s = 1$ で零点を持つことは同値になる．

「合同数をすべて決定すること」を合同数問題という．これは 10 世紀のアラビアに起源をさかのぼることができる古典的な問題であるが，現在でも完全には解決されていない．これについて，1983 年に Tunnell によって得られた次の著しい結果がある:

定理 6.4 (Tunnell の定理). n を平方因数を持たないような奇数とする．次の 2 条件を考える:

(A) n は合同数である*;*

(B) $\#\{(x,y,z) \in \mathbb{Z}^3; 2x^2 + y^2 + 8z^2 = n\}$
$= 2\#\{(x,y,z) \in \mathbb{Z}^3; 2x^2 + y^2 + 32z^2 = n\}$.

そのとき，(A) ならば (B) が成り立つ．さらに，E_n についての *BSD* 予想が正しいとすれば，(B) ならば (A) が成り立つ．

参考文献

[1] J. W. S. キャッセルズ，楕円曲線入門，1996，岩波書店．

[2] J. シルバーマン・ J. テイト，楕円曲線論入門，1995，シュプリンガー東京．

[3] 加藤和也，解決! フェルマーの最終定理，1995，日本評論社．

Mordell の定理の特別な場合の証明は，[1] と [2] に書いてある．[2] の方が読みやすいかもしれないが，[1] も高度な内容までわかりやすく解説したおもしろい本である．Fermat 予想については，日本の昔話の例え話を交えて書いてある [3] を読むことをお薦めする．楕円曲線法による素因数分解については，[1] と [2] に解説がある．