整数論の最前線

楕円曲線の数論幾何

フェルマーの最終定理，谷山–志村予想，佐藤–テイト予想，そして …

伊藤 哲史*

京都大学理学部数学教室 ガロア祭

2007年5月25日(金) 17:45–18:45

*tetsushi@math.kyoto-u.ac.jp
講演用スライドを加筆・修正したもの

この話のテーマ：楕円曲線の数論幾何

数論幾何：**整数**に関する問題を，**幾何学的手法**を使って研究．

整数は“**目に見える**”素朴な対象．目に見えている部分だけでは，
よく分からないことも多い．
より深く理解するために，“**幾何学的な視点**”を導入して研究する．

数論幾何の醍醐味

『素朴な対象の背後に，広大な世界が広がっている』

（ただし，「素朴 $\neq$ やさしい」）

最近では，ワイルズ以降，大きな進展があった．

この10年間だけでも，重要な未解決問題が数多く解かれた．

この講演では，そのうちのいくつかを(雰囲気だけでも)紹介したい．

- フェルマーの最終定理
- 谷山–志村予想
- 佐藤–テイト予想
- バーチ–スイナートン・ダイヤー予想 (BSD予想)

フェルマーの最終定理

$n \geqq 3$とすると，方程式

$$x^n + y^n = z^n$$

をみたす自然数$x, y, z \geqq 1$は存在しない．

一方，$n = 2$なら無限個存在する．

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2, \quad 7^2 + 24^2 = 25^2, \ldots$$

フェルマー(1601年～1665年)：$n = 4$の場合を証明

『私は真に驚くべき証明を見つけたが，この余白はそれを書くには狭すぎる』

フェルマーは**楕円曲線**について，深い考察を行っていた．

クンマー (1810年~1893年)

オイラー($n = 3$)，ディリクレ，ルジャンドル($n = 5$)，ラメ($n = 7$)

クンマーが**理想数**(後のイデアル)の理論により，多くのnに対して

解決(nが**正則素数**なら正しい)．

$\Rightarrow$ **代数的整数論**，**類体論**，**円分体論・岩澤理論**へと発展．

一般のnでは，フェルマーの最終定理は350年以上未解決だったが，テイラーの助けを借りて，1994年にワイルズが証明．

ワイルズによる証明

楕円曲線以外にも，モジュラー曲線，p進保型形式，ガロア表現の変形理論等の最先端の数論幾何の道具が数多く用いられた．

背理法による証明：

$a^n + b^n = c^n$とする．$\alpha = a^n,\ \beta = b^n$とおいて，

$$E : y^2 = x(x - \alpha)(x + \beta)$$

で定義された曲線(楕円曲線)を考える．

ワイルズが(部分的に)解決した谷山・志村予想によれば，この楕円曲線は保型形式に対応するはず．これはリベットの定理に矛盾する．

(証明終)

楕円曲線とは

楕円曲線とは，３次式

$$y^2 = x^3 + ax + b \qquad (4a^3 + 27b^2 \neq 0)$$

で定義された曲線のこと．

直線，２次曲線 (円，楕円，放物線，双曲線) の次に基本的な曲線．

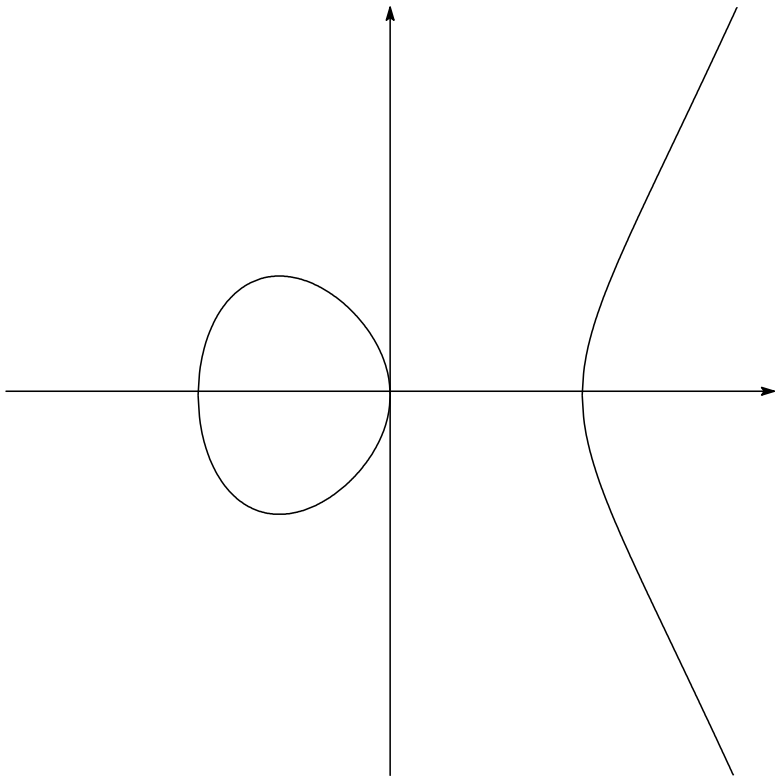
数学のいろいろな分野に顔を出す重要な対象．

(整数論，幾何学，代数幾何学，複素関数論，微分方程式，...)

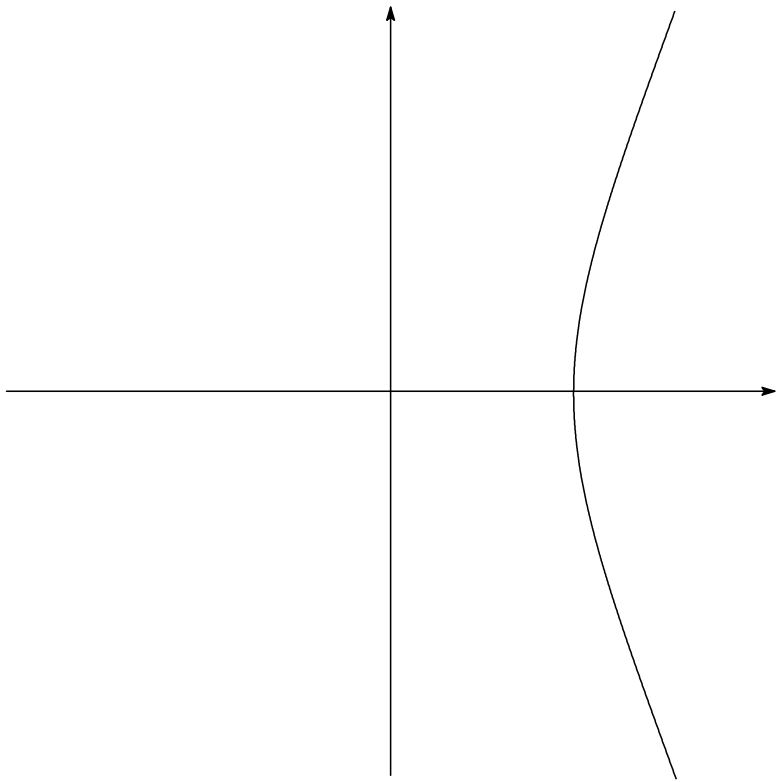
多くの数学者により深く研究されてきたが，まだまだ分からない

ことも多い．

楕円曲線のグラフ



$y^2 = x^3 - x$



$y^2 = x^3 - 4$

複素数体上では，ドーナツの形（種数１の代数曲線）．

楕円曲線についての素朴な問題

問題 ： 楕円曲線上にどのような**有理点**があるか?

言いかえると...

$$y^2 = x^3 + ax + b$$

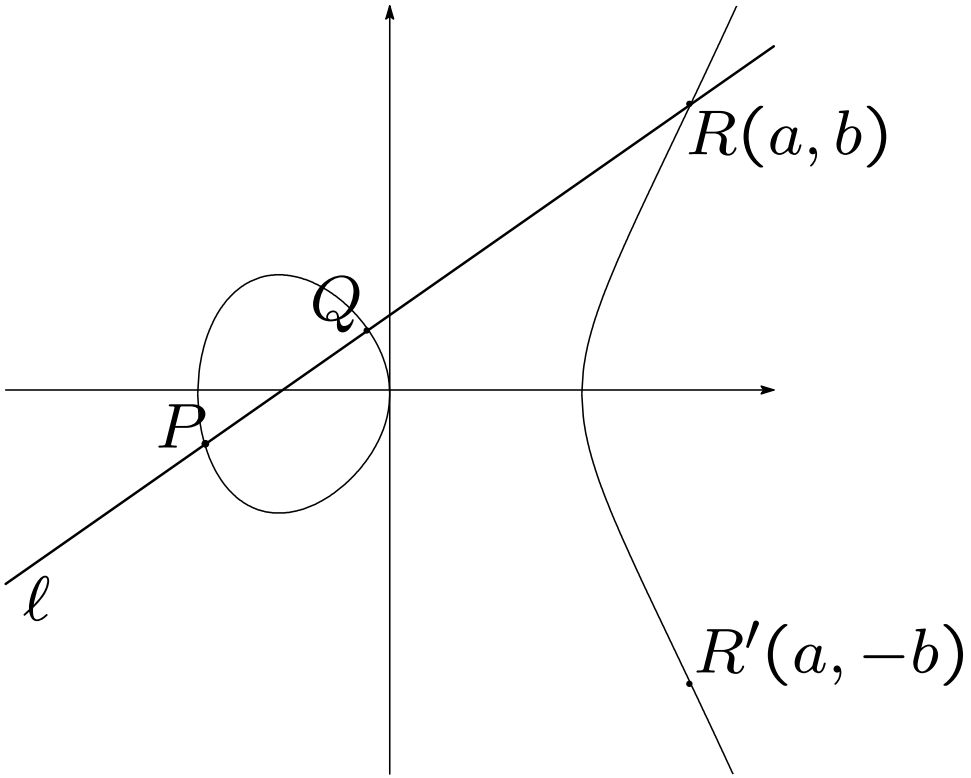
をみたす有理数x, yはどのようなものがあるか? どの位あるか?

有限個か? **無限個**か?

グラフを描いてみただけでは分からない!

素朴で重要な問題だが，いまだに完全な解答は得られていない.

3次式を幾何学的に考えてみる



ℓ : P, Q を通る直線

($P = Q$ のときは接線)

P, Q が有理点なら，

R, R' も有理点（解と係数の関係)

有理点をどんどん作っていくことができる．

この方法で，有理点を作り続けることができるか?

例 1

$E : y^2 = x^3 - 4$ 上の有理点を，$P(2,2)$ から出発して**無限個**作ることができる．

しかも，この方法で，**全ての有理点**を作ることができる．

練習問題

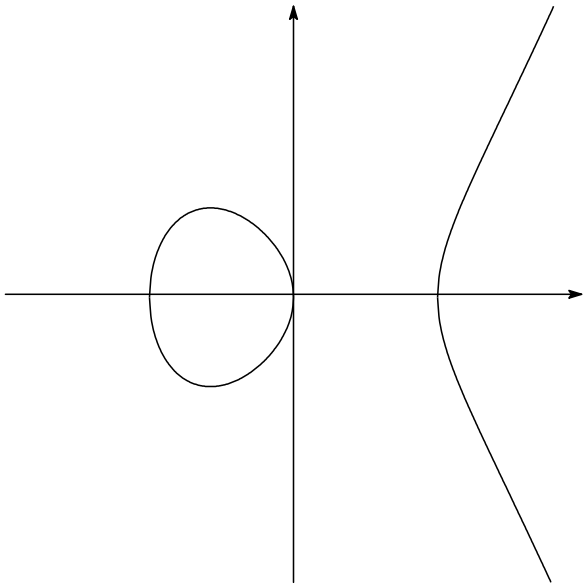
- $Q(5, \pm 11)$，$R\left(\frac{106}{9}, \pm\frac{1090}{27}\right)$，$S\left(\frac{785}{484}, \pm\frac{5497}{10648}\right)$ は E の有理点である．これらを $P(2,2)$ から作ることはできるか?

例 2 (無限に作れない例)

$E : y^2 = x^3 - x$ 上の有理点は，$(0,0)$，$(1,0)$，$(-1,0)$ のみ．

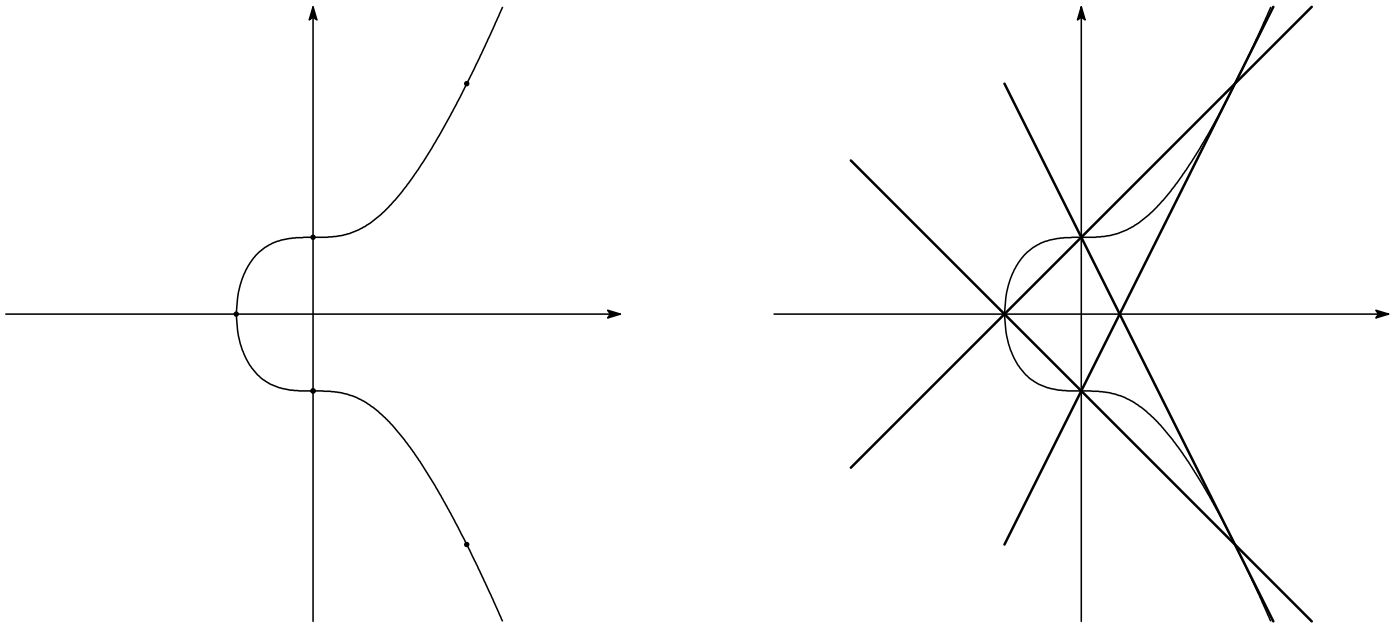
無限降下法により，フェルマーが示した．

(フェルマーの最終定理の $n = 4$ の場合と関係あり)



例 3 (無限に作れない例)

$E : y^2 = x^3 + 1$ 上の有理点は，$(-1, 0)$，$(0, \pm 1)$，$(2, \pm 3)$ のみ．



P から出発しても，有限個の有理点しか作れないとき，

P を**ねじれ点**という．

モーデルの定理 (モーデル・ヴェイユの定理)

$E : y^2 = x^3 + ax + b$ を楕円曲線とする．

このとき，有限個の有理点 $P_1, P_2, \ldots, P_n$ が存在して，

E の全ての有理点を $P_1, P_2, \ldots, P_n$ から作ることができる．

$P_1, P_2, \ldots, P_n$ を生成系という．

$Q_1, Q_2, \ldots, Q_r$ から，ねじれ点以外の有理点を全て作ることができるような r の最小値を，E の階数という．

例：$y^2 = x^3 - 4$ ： 階数１

$y^2 = x^3 - x$, $y^2 = x^3 + 1$ ： 階数０ (有理点が有限個)

問題： 整数 a, b $(4a^3 + 27b^2 \neq 0)$ が与えられた時に，楕円曲線

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

の有理点の個数が，有限個か無限個かを判定せよ．

(類題 ： 懸賞問題・問題4)

さらに，もしできることなら，

- 有限個の場合は，有理点をすべて求めよ．
- 無限個の場合は，E の階数を求めよ．また，生成系を求めよ．

次に，素数pで割った余りを考えよう

有限体 $\mathbb{F}_p$ の世界で考える：

$E : y^2 = x^3 + ax + b$を楕円曲線とする．$y^2 - (x^3 + ax + b)$ がpで割り切れるような組(x, y) $(0 \leqq x < p,\ 0 \leqq y < p)$の個数を$p$から引いたものを，$a_p(E)$とおく．

$$a_p(E) = p - \Big(y^2 - (x^3 + ax + b)\text{が}p\text{で割り切れる}(x, y)\text{の個数}\Big)$$

問：$a_p(E)$はどのような値をとるだろうか?

pを取り換えた時に，$a_p(E)$はどのように変化するだろうか?

ハッセの定理：pが$4a^3+27b^2$を割り切らなければ，

$$-2\sqrt{p} \leqq a_p(E) \leqq 2\sqrt{p}.$$

言い換え（1）：Xに関する2次方程式

$$X^2 - a_p(E)X + p = 0$$

の解の絶対値が $\sqrt{p}$ に等しい．

言い換え（2）：複素数sに関する方程式

$$1 - a_p(E)p^{-s} + p^{1-2s} = 0$$

の解をαとおくと，αの実部は $\frac{1}{2}$ に等しい．

有限体上の楕円曲線に対するリーマン予想の類似（ヴェイユ予想）．
ヴェイユ予想は，その後，グロタンディークの創始したエタール
コホモロジーを用いて，一般次元でドリーニュが解決（1974年）．

谷山-志村予想 (谷山豊，1950年代)

$E : y^2 = x^3 + ax + b$を楕円曲線とすると，

重さ2の保型形式　$f(q) = \sum_{n=1}^{\infty} b_n q^n$　が存在して，

ほとんどすべてのpに対して，$a_p(E) = b_p$が成り立つ．

例： $E : y^2 + y = x^3 - x^2$

$$
\begin{aligned}
f(q) &= q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2 \\
&= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 \\
&\quad -2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} + \cdots
\end{aligned}
$$

リベット：

谷山-志村予想が正しければ，フェルマーの最終定理も正しい．

ワイルズ：

テイラーの協力を得て，谷山-志村予想を部分的に解決．

谷山-志村予想は，その後，テイラー等により完全に解決された．

p**進保型形式と２次元ガロア表現の変形理論を使って証明．**

佐藤–テイト予想

$a_p(E) = 2\sqrt{p}\cos\theta_p(E)$ $(0 \leqq \theta_p(E) \leqq \pi)$ とおくと，$\theta_p(E)$ は

$$\frac{2}{\pi}\sin^2\theta$$

のグラフの形に分布する．(E が虚数乗法を持たなければ)

p を動かした時に，$a_p(E)$ はどのように動くかに関する予想．

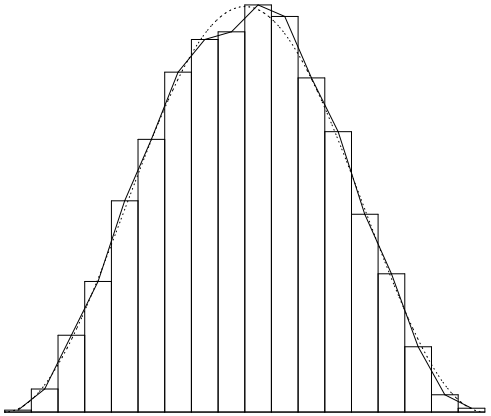
コンピュータによる計算結果を元に，1960年代初頭に佐藤幹夫が予想した．その後，テイト，セール，オッグ等が理論的根拠を与えた．

2006年春，テイラー等が，$GL(n)$ の保型表現論や n 次元ガロア表現の変形理論等を使って，(ほぼ) 解決．

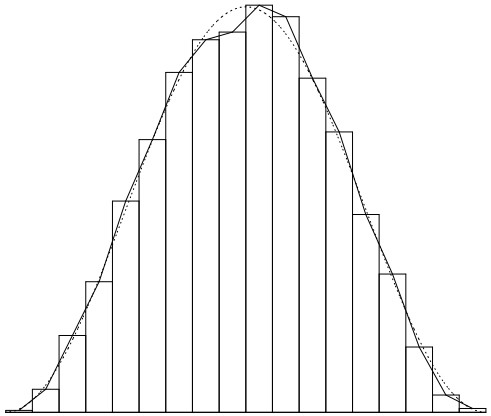
例： $E : y^2 + y = x^3 - x^2$

(11を除く)最初の1900個の素数について$\theta_p(E)$の表を作る.

$0° \le \theta < 10°$	**1**	$60° \le \theta < 70°$	**177**	$120° \le \theta < 130°$	**146**
$10° \le \theta < 20°$	**12**	$70° \le \theta < 80°$	**194**	$130° \le \theta < 140°$	**103**
$20° \le \theta < 30°$	**40**	$80° \le \theta < 90°$	**198**	$140° \le \theta < 150°$	**72**
$30° \le \theta < 40°$	**68**	$90° \le \theta < 100°$	**212**	$150° \le \theta < 160°$	**34**
$40° \le \theta < 50°$	**110**	$100° \le \theta < 110°$	**206**	$160° \le \theta < 170°$	**9**
$50° \le \theta < 60°$	**142**	$110° \le \theta < 120°$	**174**	$170° \le \theta \le 180°$	**2**



ところで…



と

は似てる？

それはさておき...

ここまでのまとめ：

- 楕円曲線$E : y^2 = x^3 + ax + b$の有理点は，有限個かもしれないし，無限個かもしれない．
- 有限個の有理点$P_1, \ldots, P_n$をうまく選べば，Eの有理点を全て作ることができる．(モーデルの定理)
- $a_p(E) = p - \left(y^2 - (x^3 + ax + b)\right.$が$p$で割り切れる$\left.(x, y)\text{の個数}\right)$とおくと，$-2\sqrt{p} \leqq a_p(E) \leqq 2\sqrt{p}$．(ハッセの定理)
- $a_p(E)$は重さ２の保型形式のFourier係数と一致する．(谷山-志村予想)
- $a_p(E) = 2\sqrt{p}\cos\theta_p(E)$とおくと，$\theta_p(E)$の分布は$\frac{2}{\pi}\sin^2\theta$の形．($E$が虚数乗法を持たなければ)（佐藤-テイト予想)

問： $a_p(E)$ と E の有理点の間に，関係はあるのか?

21世紀の大予想：バーチ-スイナートン・ダイヤー予想

クレイ数学研究所の7つの100万ドル懸賞金問題のうちの1つ．

楕円曲線$E : y^2 = x^3 + ax + b$のL関数を

$$L(s, E) = \prod_{p\ :\ \text{素数}} \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}}$$

で定める．(pが$4a^3 + 27b^2$を割り切る時は，修正が必要)

谷山-志村予想により，$L(s, E)$は複素平面全体に解析接続される．

予想：$\left(\ L(s, E)\text{の}s = 1\text{での位数}\ \right) = \left(\ E\text{の階数}\ \right)$

特に，Eの有理点が有限個であることと，$L(1, E) \neq 0$は同値．

多くの数学者により活発に研究されているが，一般には未解決．

定理(コーツ-ワイルズ，1977年)：Eが虚数乗法を持つとする．

$L(1,E) \neq 0$ならば，Eの有理点は有限個．

定理(グロス-ザギエー，コリヴァギン，ルビン，1980年代)：

$L(1,E) \neq 0$または$L'(1,E) \neq 0$なら，BSD予想は正しい．

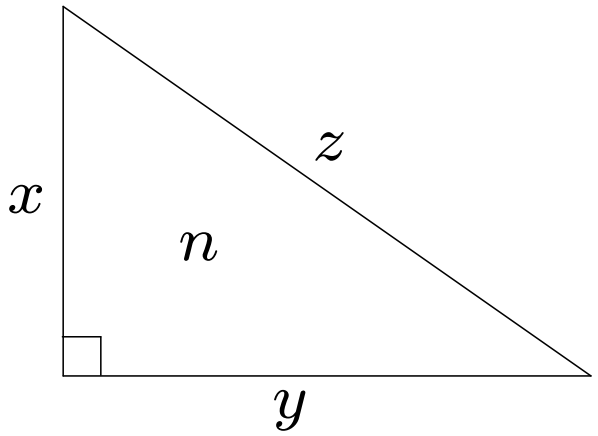
階数$\geqq 2$の場合は，ほとんど何もわかっていない．

定理(加藤和也，1990年代)：

$\left(\ p\text{進}L\text{関数}L_p(s,E)\text{の}s=1\text{での位数}\ \right) \geqq \left(\ E\text{の階数}\ \right)$

最後に，素朴な話に戻ろう

問題：nを自然数とする．３辺が有理数の直角二等辺三角形で，
面積がnのものが存在するかどうかを判定せよ．
(存在するとき，nを**合同数**という)

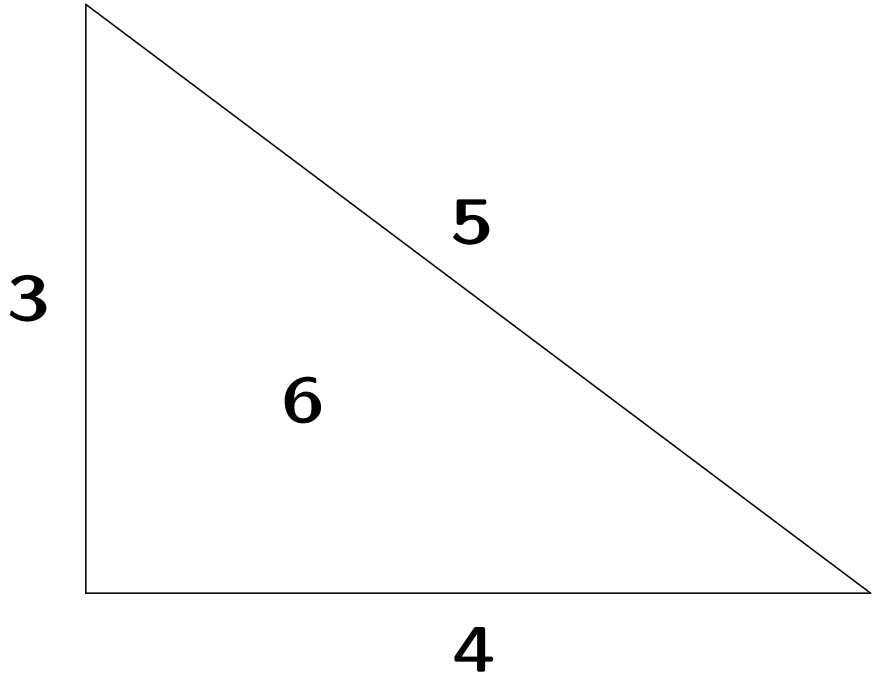


$$x^2 + y^2 = z^2$$

$$\frac{1}{2}xy = n$$

中学生でも思いつきそうな素朴な問題．少なくとも1000年以上研究されている．合同数の例は？ 合同数でない自然数は？

例１：６は合同数である

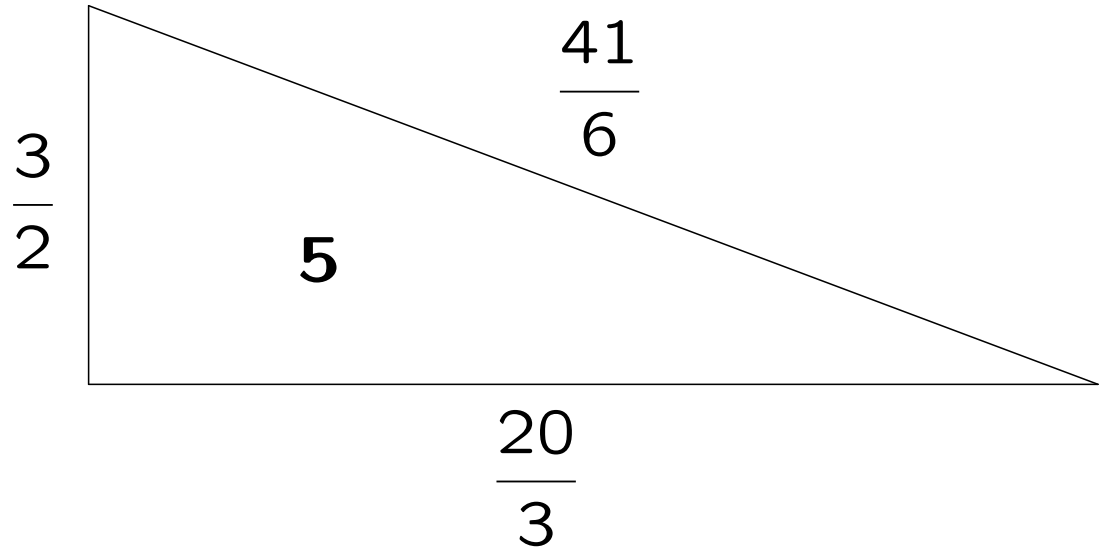


$$3^2 + 4^2 = 5^2$$

$$\frac{1}{2} \times 3 \times 4 = 6$$

問：では，５は合同数だろうか?

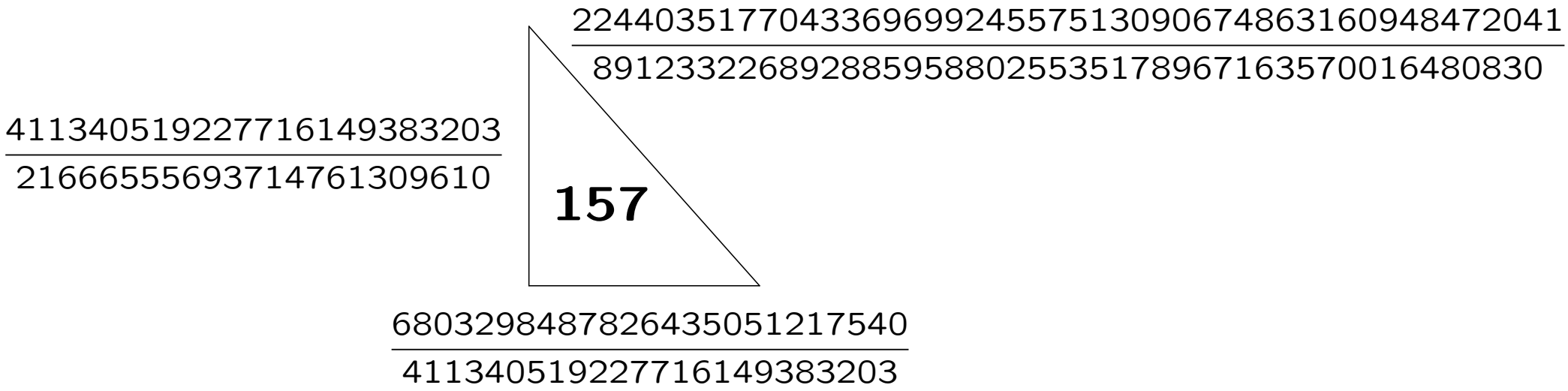
例２：５は合同数である



演習問題：７が合同数であることを示せ．

(残念ながら，賞品は出ませんが…)

例３：157は合同数である



例４：１は合同数ではない!

証明：有理数$a, b, c > 0$に対し，$a^2 + b^2 = c^2$, $\frac{1}{2}ab = 1$と仮定する．$a \neq b$である．

$\alpha = \frac{c^2}{4}$, $\beta = \frac{(a^2-b^2)c}{8}$とおくと，

$$\alpha^3 - \alpha = \frac{c^2(c^4 - 16)}{64} = \frac{c^2}{64}\left\{(a^2 + b^2)^2 - 16\left(\frac{1}{2}ab\right)^2\right\}$$
$$= \frac{c^2(a^2 - b^2)^2}{64} = \beta^2$$

なので(α, β)が楕円曲線$y^2 = x^3 - x$の$y \neq 0$となる有理点を与える．これはフェルマーが証明した事実に反する．　(証明終)

合同数を判定することはできるか?

合同数判定予想：$n \geq 1$を**奇数**で，平方数で割れないとすると，

次の (1),(2) は同値である．

(1) nは **合同数** である．

(2) 「$n = 2x^2 + y^2 + 32z^2$の整数解の個数」の２倍が，

「$n = 2x^2 + y^2 + 8z^2$ の整数解の個数」に等しい．

※ (2) は，具体的に計算して確かめることができるが，

(1) は，(一見すると) そうではない．

演習問題：この予想を確かめてみよう．

- $n = 5, 6, 7, 157$ は合同数である．
- $n = 1$ は合同数ではない．
- $n = 41$ は合同数だろうか?

「$n = 2x^2 + y^2 + 32z^2$ の整数解の個数」の２倍

$\stackrel{?}{=}$ 「$n = 2x^2 + y^2 + 8z^2$ の整数解の個数」

タンネルの定理 (1983年)

- 「(1) $\Rightarrow$ (2)」 が成り立つ．つまり，nが**合同数**なら，

  「$n = 2x^2 + y^2 + 32z^2$ の整数解の個数」の２倍が，

  「$n = 2x^2 + y^2 + 8z^2$ の整数解の個数」に等しい．

- **もしBSD予想が正しければ**,「(2) $\Rightarrow$ (1)」 も成り立つ．

例 ($n = 11$)：

$11 = 2x^2 + y^2 + 32z^2 \cdots (x, y, z) = (\pm 1, \pm 3, 0)$ (4個)

$11 = 2x^2 + y^2 + 8z^2 \cdots (\pm 1, \pm 3, 0), (\pm 1, \pm 1, \pm 1)$ (12個)

$4 \times 2 \neq 12$なので，タンネルの定理より，**11は合同数ではない**．

タンネルの証明から,「$(2) \Rightarrow (1)$」は,

(特別な場合の) BSD予想と同値であることも分かる.

つまり,合同数判定予想はBSD予想と同じ位難しい!

タンネルの定理の証明は,当時の数論幾何・保型形式論の最先端の結果を駆使したものだった.

- コーツ-ワイルズの定理 (BSD予想の部分的解決)
- テータ関数,重さ$k+\frac{1}{2}$の保型形式 (志村対応)
- ヴァルジュプルジェーの定理 (L関数の特殊値の計算)

『素朴な対象の背後に,広大な世界が広がっている』