For Tutors

MeBio　数学テキスト

王城夕紀「青の数学」の問題

—問題と解答—

Edited by kamei

第 1 章

問題

§ 1　問題

子供に借りて王城夕紀「青の数学」という小説を読んでいます．数学に打ち込む少年達を描いたさわやかな青春小説ですが，載っている問題に数学オリンピックレベルのものがありました．解かないまま先を読む気はしなかったのでしばらく停滞してしまいましたが，解決したので書き残しておきます．

問題 1–1–1　$x^2 \pm (x+y+z)$, $y^2 \pm (x+y+z)$, $z^2 \pm (x+y+z)$ がどれも有理数の平方であるような正の有理数 $x,\ y,\ z$ を一組求めよ．

小説に載っていた解答　$(x,\ y,\ z) = \left(\dfrac{203}{48},\ \dfrac{259}{48},\ \dfrac{791}{96} \right)$

亀井が見つけた解答

$x,\ y,\ z$ がすべて異なっている例としては，$(x,\ y,\ z) = \left(\dfrac{17848817}{341880},\ \dfrac{3560413}{170940},\ \dfrac{861193}{341880} \right)$,
$\left(\dfrac{397781}{55440},\ \dfrac{476033}{110880},\ \dfrac{7909973}{1164240} \right)$, $\left(\dfrac{265523}{26208},\ \dfrac{1140187}{78624},\ \dfrac{16759187}{2620800} \right)$, $\left(\dfrac{642667}{110880},\ \dfrac{1318171}{221760},\ \dfrac{7097483}{332640} \right)$
などなど．解は無限に存在する．無限個の例を作ることが出来る．

この問題は，合同数 n に付随する楕円曲線 $X^3 - X = nY^2$ の異なる 3 つの有理点を求めることに帰着する，従ってすべての解を表示することは不可能なのだが，弱 BSD 予想が正しいなら Tunnel の定理の逆が成り立つので n が合同数であるかないかの判定が出来ることになり，解の列挙が（原理的には）可能となる．ただしヒーグナー点に関するグロス–ザギエの定理などを必要とする．解自体もすさまじい桁のものばかりとなる．

$x,\ y,\ z$ のうち等しいものが存在してもよい場合，例えば $(x,\ x,\ x)$ が解であるためには，m を $1+\sqrt{2}$ 以上の有理数として $x = \dfrac{3(m^2+1)^2}{4(m-1)m(m+1)}$ と書かれることが必要十分であると証明できる．

□

第 2 章

解法

§ 1　写像 $F:(x,\ y,\ z)\mapsto(m_x,\ m_y,\ m_z)$ の構成

題意を満たす $x,\ y,\ z$ が存在したとする．$x^2+(x+y+z)={R_x}^2$, $x^2-(x+y+z)={r_x}^2$ と置く．辺々足すと $2x^2={R_x}^2+{r_x}^2$ つまり

$$\left(\frac{R_x}{x}\right)^2+\left(\frac{r_x}{x}\right)^2=2$$

が得られる．これは $\left(\dfrac{R_x}{x},\ \dfrac{r_x}{x}\right)$ が XY 平面の円 $X^2+Y^2=2$ 上の有理点であることを表す．

$\left(0<\dfrac{r_x}{x}<1<\dfrac{R_x}{x}<\sqrt{2}\text{ の範囲にある．}\right)$　これより $\dfrac{R_x}{x},\ \dfrac{r_x}{x}$ をパラメータ $m_x\in\mathbb{Q}$ で表示することが可能であると気付く．

本問の場合は，$0<\dfrac{r_x}{x}<\dfrac{R_x}{x}$ の有理点を都合よく表すために，

$$\left(\frac{R_x}{x},\ \frac{r_x}{x}\right)=\left(\frac{{m_x}^2+2m_x-1}{{m_x}^2+1},\ \frac{{m_x}^2-2m_x-1}{{m_x}^2+1}\right)\tag{2.1}$$

というパラメータ表示を採用する．この m_x は何かの傾きそのものではない．$\left(\dfrac{R_x}{x},\ \dfrac{r_x}{x}\right)$ と $(-1,\ -1)$ を通る直線が $x+y+2=0$ となす角を θ とすると，$m_x=\tan\theta$ となっている．

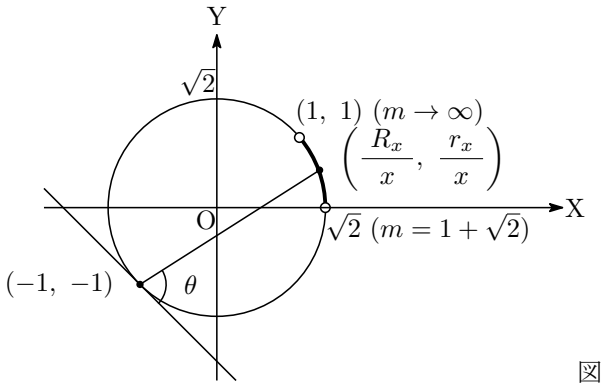


図 1

具体的に m_x を $x,\ R_x,\ r_x$ で表すと

$$m_x=\frac{-\dfrac{R_x}{x}+\dfrac{r_x}{x}}{\dfrac{R_x}{x}+\dfrac{r_x}{x}-2}=\frac{R_x-r_x}{2x-R_x-r_x}\tag{2.2}$$

となる．m_x は $1+\sqrt{2}$ より大きな有理数である．$m_y,\ m_z$ も同様に決めることが出来る．

題意を満たす正の有理数の組の集合を S としよう．

$$S = \{(x,\ y,\ z) \in {\mathbb{Q}_+}^3 \mid x^2 \pm (x+y+z) \in (\mathbb{Q}_+)^2,\ y^2 \pm (x+y+z) \in (\mathbb{Q}_+)^2,\ z^2 \pm (x+y+z) \in (\mathbb{Q}_+)^2\}$$

である．[1] また

$$M = \{(m_x,\ m_y,\ m_z) \in \mathbb{Q}^3 \mid m_x > 1+\sqrt{2},\ m_y > 1+\sqrt{2},\ m_z > 1+\sqrt{2}\}$$

と置く．M は $1+\sqrt{2}$ より大きい 3 つの有理数の組の集合である．

今までの考察により $(x,\ y,\ z) \in S$ から $1+\sqrt{2}$ より大きい有理数の組 $(m_x,\ m_y,\ m_z) \in M$ を決定する関数

$$F : S \to M;\ F(x,\ y,\ z) = (m_x,\ m_y,\ m_z)$$

を構成することが出来た．[2]

例 2.1 小説に載っていた答の $(x,\ y,\ z) = \left(\dfrac{203}{48},\ \dfrac{259}{48},\ \dfrac{791}{96}\right)$ を使って具体的に説明しておく．

$x+y+z = \dfrac{1715}{96}$ であり，

$$\begin{aligned} R_x &= \sqrt{x^2+(x+y+z)} = \sqrt{\frac{41209}{2304}+\frac{1715}{96}} = \sqrt{\frac{82369}{2304}} = \frac{287}{48}, \\ r_x &= \sqrt{x^2-(x+y+z)} = \sqrt{\frac{41209}{2304}-\frac{1715}{96}} = \sqrt{\frac{49}{2304}} = \frac{7}{48} \end{aligned}$$

である．$m_x = \dfrac{R_x - r_x}{2x - R_x - r_x} = \dfrac{\dfrac{287}{48} - \dfrac{7}{48}}{2\cdot\dfrac{203}{48} - \dfrac{287}{48} - \dfrac{7}{48}} = \dfrac{5}{2}$ であり，

$$\left(\frac{R_x}{x},\ \frac{r_x}{x}\right) = \left(\frac{287}{203},\ \frac{7}{203}\right) = \left(\frac{41}{29},\ \frac{1}{29}\right) = \left(\frac{{m_x}^2+2m_x-1}{{m_x}^2+1},\ \frac{{m_x}^2-2m_x-1}{{m_x}^2+1}\right)$$

が確かに成り立っていることがわかる．

□

§ 2　$(m_x,\ m_y,\ m_z)$ の満たす性質

$(m_x,\ m_y,\ m_z) \in M$ から F の逆元 $(x,\ y,\ z) = F^{-1}(m_x,\ m_y,\ m_z)$ を求めたいのだが，3 数 $m_x,\ m_y,\ m_z$ を勝手に決めたのでは $(x,\ y,\ z)$ は存在しないだろう．要するに F は全射ではないであろう．像 $F(S)$，つまりこれら 3 数の満たすべき条件を求めておきたい．

ある $(x,\ y,\ z) \in S$ に対して $(m_x,\ m_y,\ m_z) = F(x,\ y,\ z)$ であるとする．(2.1) より

$$R_x = \frac{{m_x}^2+2m_x-1}{{m_x}^2+1}x,\ r_x = \frac{{m_x}^2-2m_x-1}{{m_x}^2+1}x,$$

であるから，これを代入して

$$x+y+z = {R_x}^2 - x^2 = x^2 - {r_x}^2 = \frac{4x^2(m_x-1)m_x(m_x+1)}{({m_x}^2+1)^2}$$

であることがわかる．$y,\ z$ に関しても同様だから，次が成立している．

---

[1] ${\mathbb{Q}_+}^3 = \mathbb{Q}_+ \times \mathbb{Q}_+ \times \mathbb{Q}_+$ （直積集合）であるが，$(\mathbb{Q}_+)^2$ は $\mathbb{Q}_+ \times \mathbb{Q}_+$ ではなく，$\{x^2 \mid x \in \mathbb{Q}_+\}$ を意味している．

[2] x だけから m_x を決めることは出来ない．$x+y+z$ が決まらないと $R_x,\ r_x$ が決まらないからである．

命題 2.2

$$x+y+z=\frac{4x^2(m_x-1)m_x(m_x+1)}{({m_x}^2+1)^2}=\frac{4x^2(m_y-1)m_y(m_y+1)}{({m_y}^2+1)^2}=\frac{4x^2(m_z-1)m_z(m_z+1)}{({m_z}^2+1)^2} \tag{2.3}$$

□

定義 2.3 $r\in\mathbb{Q}_+$ はある有理数係数の直角三角形の面積になり得るとき，合同数と呼ぶ.

$$\begin{aligned} & r\in\mathbb{Q}_+ \text{ が合同数} \\ \iff\quad & x^2=y^2+z^2,\ r=\frac{yz}{2}\ (x,\ y,\ z,\ r\in\mathbb{Q}_+) \text{ が解を持つ} \end{aligned}$$

斜辺が x の直角三角形の他の二辺は $y=\dfrac{m^2-1}{m^2+1}x,\ z=\dfrac{2m}{m^2+1}x\ (m\in\mathbb{Q}_{>1+\sqrt{2}})$ と表すことが出来る．その場合面積は $\dfrac{yz}{2}=\dfrac{m(m^2-1)x^2}{(m^2+1)^2}$ であるから，次のようにいってもよい.

$$r\in\mathbb{Q}_+ \text{ が合同数} \quad\iff\quad r=\frac{m(m^2-1)x^2}{(m^2+1)^2} \text{ が解を持つ}$$

□

$m(m^2-1)$ を m が定める合同数と呼ぶことにすると，命題 2.2 は次のように言い換えられる.

命題 2.4 $x+y+z$ と $m_x,\ m_y,\ m_z$ の定める合同数は平方因子の違いしかない．つまり乗法群 $\mathbb{Q}_+$ において

$$x+y+z\equiv(m_x-1)m_x(m_x+1)\equiv(m_y-1)m_y(m_y+1)\equiv(m_z-1)m_z(m_z+1)\mod(\mathbb{Q}_+)^2$$

□

どのような有理数が合同数であるかに関しては，次の章で考察する.

命題 2.2 から $x:y:z$ の比が決まる.

$$x:y:z=\frac{{m_x}^2+1}{2\sqrt{(m_x-1)m_x(m_x+1)}}:\frac{{m_y}^2+1}{2\sqrt{(m_y-1)m_y(m_y+1)}}:\frac{{m_z}^2+1}{2\sqrt{(m_z-1)m_z(m_z+1)}} \tag{2.4}$$

命題 2.4 よりこの比は有理比になる.
そのあたりの事情を把握するためには $\mathbb{Q}_+/(\mathbb{Q}_+)^2$ の代表元を与える関数を導入しておくと便利がよい.

定義 2.5 正の有理数 m に対し，$m \mod(\mathbb{Q}_+)^2$ の代表元 $\mu(m)$ を，$m\equiv\mu(m) \mod(\mathbb{Q}_+)^2$ が成り立つ最小の自然数とする．それを使って $\varphi(m)=\mu((m-1)m(m+1))$ と定義する. □

例えば $\mu\left(\dfrac{2\cdot3^2}{5^3\cdot7^4}\right)=\mu\left(\left(\dfrac{3}{5^2\cdot7^2}\right)^2\times2\cdot5\right)=2\cdot5$ である．要するに $\mu(m)$ は，m の分母であろうが分子であろうが，奇数次で登場する素因数をすべて 1 回ずつかけたものと定義するのである．また，
$\varphi\left(\dfrac{7}{2}\right)=\mu\left(\dfrac{5}{2}\cdot\dfrac{7}{2}\cdot\dfrac{9}{2}\right)=2\cdot5\cdot7$ である.

この記号を用いると，$m_x,\ m_y,\ m_z$ の満たすべき条件は次のように表現できる.

命題 2.6 $(x,\ y,\ z)\in S$ から誘導された $(m_x,\ m_y,\ m_z)=F(x,\ y,\ z)$ は $\varphi(m_x)=\varphi(m_y)=\varphi(m_z)$ を満たす.

□

§ 3　$(m_x,\ m_y,\ m_z)$ から $(x,\ y,\ z)$ を復元する

あらゆる有理数 r に対して $\dfrac{r}{\mu(r)}$ は有理数の平方だから，$\sqrt{\dfrac{\varphi(m)}{(m-1)m(m+1)}} = \sqrt{\dfrac{\mu((m-1)m(m+1))}{(m-1)m(m+1)}} \in \mathbb{Q}$ である．そこで $m > 1+\sqrt{2}$ を満たす有理数 m に対して $\psi(m) \in \mathbb{Q}_+$ を

$$\psi(m) = \frac{m^2+1}{2}\sqrt{\frac{\varphi(m)}{(m-1)m(m+1)}}$$

と定義する．$\varphi(m)$ を使って $(m-1)m(m+1)$ の非平方因子を取り除くのである．これにより，$x:y:z$ を有理数の比として表すことが出来る，結果は次の通り．

系 2.7 $(x,\ y,\ z) \in S$ から誘導された $(m_x,\ m_y,\ m_z) = F(x,\ y,\ z)$ に対して

$$x:y:z = \psi(m_x):\psi(m_y):\psi(m_z)$$

が成り立っている．　□

例 2.8 先程と同じく $(x,\ y,\ z) = \left(\dfrac{203}{48},\ \dfrac{259}{48},\ \dfrac{791}{96}\right)$ を使おう．$m_x = \dfrac{5}{2}$ であった．

$(m_x-1)m_x(m_x+1) = \dfrac{3}{2}\cdot\dfrac{5}{2}\cdot\dfrac{7}{2} = \left(\dfrac{1}{2}\right)^2\cdot 2\cdot 3\cdot 5\cdot 7$ だから $\varphi(m_x) = 2\cdot 3\cdot 5\cdot 7$ であり，

$$\psi(m_x) = \frac{{m_x}^2+1}{2}\sqrt{\frac{\varphi(m_x)}{(m_x-1)m_x(m_x+1)}} = \frac{\left(\dfrac{5}{2}\right)^2+1}{2}\sqrt{\frac{2\cdot 3\cdot 5\cdot 7}{\dfrac{3}{2}\cdot\dfrac{5}{2}\cdot\dfrac{7}{2}}} = \frac{29}{2}$$

となる．y に関しても同様に

$R_y = \sqrt{y^2+(x+y+z)} = \dfrac{329}{48}$, $r_y = \sqrt{y^2-(x+y+z)} = \dfrac{161}{48}$, $m_y = \dfrac{R_y - r_y}{2y - R_y - r_y} = 6$,

$(m_y-1)m_y(m_y+1) = 5\cdot 6\cdot 7 = 2\cdot 3\cdot 5\cdot 7$, $\varphi(m_y) = 2\cdot 3\cdot 5\cdot 7$ であり，

$$\psi(m_y) = \frac{{m_y}^2+1}{2}\sqrt{\frac{\varphi(m_y)}{(m_y-1)m_y(m_y+1)}} = \frac{6^2+1}{2}\sqrt{\frac{2\cdot 3\cdot 5\cdot 7}{2\cdot 3\cdot 5\cdot 7}} = \frac{37}{2}$$

となる．z に関しては

$R_z = \sqrt{z^2+(x+y+z)} = \dfrac{889}{96}$, $r_z = \sqrt{z^2-(x+y+z)} = \dfrac{679}{48}$, $m_z = \dfrac{R_z - r_z}{2z - R_z - r_z} = 15$,

$(m_z-1)m_z(m_z+1) = 14\cdot 15\cdot 16 = 2^5\cdot 3\cdot 5\cdot 7$, $\varphi(m_z) = 2\cdot 3\cdot 5\cdot 7\cdot$ であり，

$$\psi(m_z) = \frac{{m_z}^2+1}{2}\sqrt{\frac{\varphi(m_z)}{(m_z-1)m_z(m_z+1)}} = \frac{15^2+1}{2}\sqrt{\frac{2\cdot 3\cdot 5\cdot 7}{2^5\cdot 3\cdot 5\cdot 7}} = \frac{113}{4}$$

となる．以上より

$$\psi(m_x):\psi(m_y):\psi(m_z) = \frac{29}{2}:\frac{37}{2}:\frac{113}{4} = 58:74:113$$

であり，これは $x:y:z = \dfrac{203}{48}:\dfrac{259}{48}:\dfrac{791}{96} = 58:74:113$ に一致している．　□

定理 2.9 $1+\sqrt{2}$ より大きい 3 つの有理数 $m_x,\ m_y,\ m_z$ が $\varphi(m_x) = \varphi(m_y) = \varphi(m_z)$ を満たすとしよう．そのとき題意を満たす $(x,\ y,\ z)$ で $F(x,\ y,\ z) = (m_x,\ m_y,\ m_z)$ を満たすものがただ一つ存在する．つまり

$$M_0 = \{(m_x,\ m_y,\ m_z) \in M \mid \varphi(m_x) = \varphi(m_y) = \varphi(m_z)\}$$

とすると $F : S \to M_0$ は全単射で，F^{-1} が存在する．

証明　$(x,\ y,\ z)$ が存在するのであれば，それらは系 2.7 を満たさないといけないので，ある正の有理数 k が存在して

$$x = k\psi(m_x),\ y = k\psi(m_y),\ z = k\psi(m_z)$$

と表されるはずである．これら $x,\ y,\ z$ はさらに命題 2.2 も満たさないといけないので

$$k\psi(m_x) + k\psi(m_y) + k\psi(m_z) = \frac{4k^2\psi(m_x)^2(m_x-1)m_x(m_x+1)}{({m_x}^2+1)^2} = k^2\varphi(m_x)$$

$$\left(\because \psi(m_x) = \frac{{m_x}^2+1}{2}\sqrt{\frac{\varphi(m_x)}{(m_x-1)m_x(m_x+1)}}\right)$$

従って k は $k = \dfrac{\psi(m_x)+\psi(m_y)+\psi(m_z)}{\varphi(m_x)}$ と一意に決まってしまう．この $(x,\ y,\ z)$ は (2.3) を満たすので，

$$\begin{aligned} & x^2 + (x+y+z) \\ = \ & x^2 + \frac{4x^2(m_x-1)m_x(m_x+1)}{({m_x}^2+1)^2} \\ = \ & \frac{{m_x}^4 + 2{m_x}^2 + 1 + 4{m_x}^3 - 4m_x}{({m_x}^2+1)^2}x^2 \\ = \ & \left(\frac{{m_x}^2 + 2m_x - 1}{{m_x}^2+1}x\right)^2 \end{aligned}$$

などが成り立つことが確かめられる．つまりこの $(x,\ y,\ z)$ は S に含まれていて $F(x,\ y,\ z) = (m_x,\ m_y,\ m_z)$ を満たす．　□

例 2.10　またまた $(x,\ y,\ z) = \left(\dfrac{203}{48},\ \dfrac{259}{48},\ \dfrac{791}{96}\right)$ を使おう．ただし今回はこの $(x,\ y,\ z)$ の存在は未知であるものとし，$(m_x,\ m_y,\ m_z) = \left(\dfrac{5}{2},\ 6,\ 15\right)$ が $\varphi(m_x) = \varphi(m_y) = \varphi(m_z)(= 2\cdot 3\cdot 5\cdot 7)$ を満たすことだけから $(x,\ y,\ z)$ を復元させてみる．例 2.8 で計算したように $\psi(m_x) = \dfrac{29}{2}$, $\psi(m_y) = \dfrac{37}{2}$, $\psi(m_z) = \dfrac{113}{4}$ だったから

$$k = \frac{\psi(m_x)+\psi(m_y)+\psi(m_z)}{\varphi(m_x)} = \frac{\dfrac{29}{2}+\dfrac{37}{2}+\dfrac{113}{4}}{2\cdot 3\cdot 5\cdot 7} = \frac{7}{24}$$

これより

$$(x,\ y,\ z) = k(\psi(m_x),\ \psi(m_y),\ \psi(m_z)) = \frac{7}{24}\left(\frac{29}{2},\ \frac{37}{2},\ \frac{113}{4}\right) = \left(\frac{203}{48},\ \frac{259}{48},\ \frac{791}{96}\right)$$

となり，確かに元の $(x,\ y,\ z)$ が復元されている．　□

§ 4　楕円関数の有理点

ここまでの結果により，題意を満たす $(x,\ y,\ z)$ を見つけることは $(m_x,\ m_y,\ m_z) \in M_0$ を見つけることと同値になった．有理数 m に対して $\varphi(m)$ を計算するのは非常に容易なので，最初は多くの $m(> 1+\sqrt{2})$ に対して $\varphi(m)$ を計算して，$\varphi(m)$ の値が同じものを 3 つ集めたのだが，その後もっと本質的な方法に気付いた．

定理 2.11 m_1 を $1+\sqrt{2}$ より大きな有理数とし，$\varphi(m_1)=n$ とする．$\varphi(m)=n$ を満たす $1+\sqrt{2}$ より大きな有理数 m は無限に存在する．

証明 $\varphi(m_1)=n$ だから $m^3-m=nx^2$ はある有理数解 (m_1, x_1) を持つ．つまり $(X,\ Y)=(m_1,\ x_1)$ は楕円曲線 $X^3-X=nY^2$ の有理点である．しかもこの有理点は無限位数を持つことが容易にわかる．(torsion は $(0,\ 0),\ (1,\ 0),\ (-1,\ 0)$ だけである．)

別の有理数解を $(X,\ Y)=(m_2,\ x_2)$ とする．$m_2>1+\sqrt{2}$ ならそのまま $\varphi(m_2)=n$ が成り立つ．$1<m_2<1+\sqrt{2}$ なら $m'=\dfrac{m_2+1}{m_2-1}$ と置くと $\varphi(m')=n$ が成り立つ．

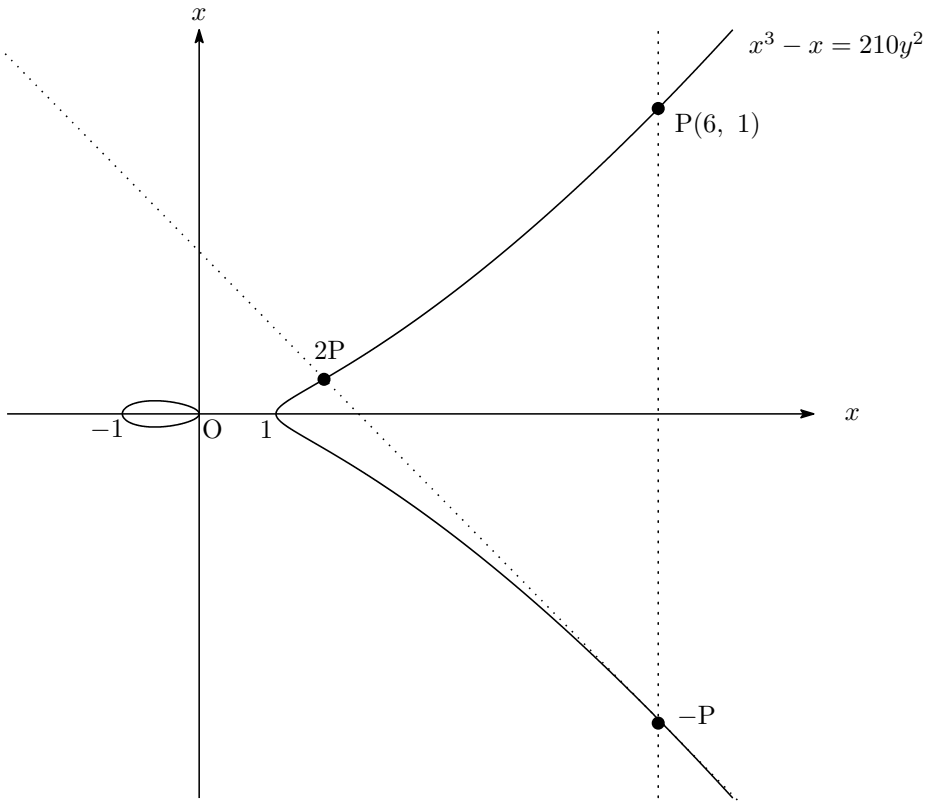
$\because$ 図 1 で $m_2=\tan\theta,\ m'=\tan\theta'$ と置くと $\dfrac{\theta+\theta'}{2}=\dfrac{3}{8}\pi$ になっている．つまり m_2 の定める円周上の点と m' の定める円周上の点は X 軸対象の位置にある．従って $\tan\theta'=\tan\left(\dfrac{3}{4}\pi-\theta\right)=\dfrac{\tan\dfrac{3}{4}\pi-\tan\theta}{1+\tan\dfrac{3}{4}\pi\cdot\tan\theta}$

$=\dfrac{-1-m_2}{1-m_2}=\dfrac{m_2+1}{m_2-1}$ である．このとき $(m'-1)m'(m'+1)=\left(\dfrac{m_2+1}{m_2-1}-1\right)\dfrac{m_2+1}{m_2-1}\left(\dfrac{m_2+1}{m_2-1}+1\right)$

$=\dfrac{2\cdot(m_2+1)\cdot 2m_2}{(m_2-1)^3}=\left\{\dfrac{2}{(m_2-1)^2}\right\}^2(m_2-1)m_2(m_2+1)$ だから $\varphi(m')=\varphi(m_2)$ が成り立っている．

□

例 2.12 $\varphi(6)=\mu(5\cdot6\cdot7)=2\cdot3\cdot5\cdot7=210$ である．$(6,\ 1)$ は楕円曲線 $E: X^3-X=210Y^2$ の有理点である．この点を P とする，



$(\infty,\ \infty)$ を 0 として，$E(\mathbb{Q})$ に通常通りの群構造が入る，P の逆元は $-\mathrm{P}(6,\ -1)$ である．

$-\mathrm{P}$ における E の接線は $Y=\dfrac{107}{420}(X-6)-1$ であり，この接線と E の交点が $2\mathrm{P}\left(\dfrac{1369}{840},\ \dfrac{39997}{352800}\right)$ である．

2P は E 上の点であり $\dfrac{1369}{840} > 1+\sqrt{2}$ だから $\varphi\left(\dfrac{1369}{840}\right) = 210$ が成り立つ．実際

$$\left(\frac{1369}{840}-1\right)\left(\frac{1369}{840}\right)\left(\frac{1369}{840}+1\right) = \frac{23^2\cdot 37^2\cdot 47^2}{2^9\cdot 3^3\cdot 5^3\cdot 7^3} \equiv 2\cdot 3\cdot 5\cdot 7 = 210$$

次に $-\mathrm{P}(6,1)$, $-2\mathrm{P}\left(\dfrac{1369}{840},\ -\dfrac{39997}{352800}\right)$ を通る直線を考える．3 次方程式

$$X^3 - X = 210\left\{\frac{-\dfrac{39997}{352800}-(-1)}{\dfrac{1369}{840}-6}(X-6)-1\right\}^2$$

が $X=6$, $X=\dfrac{1369}{840}$ を解に持つことより 3 つめの解が計算できる．これより $3\mathrm{P}\left(\dfrac{13662486}{13476241},\ \dfrac{573445653}{49471280711}\right)$ を得る．

この場合の $m=\dfrac{13662486}{13476241}$ は $m>1+\sqrt{2}$ を満たしていないのだが $m'=\dfrac{m+1}{m-1}=\dfrac{27138727}{186245}$ が $m'>1+\sqrt{2}$ を満たしており，$\varphi(m')=n$ である．

計算を進めると

$$4\mathrm{P}\quad \left(\frac{6655166817121}{5375193630240},\ -\frac{10123232905622052719}{180592960488115795200}\right)$$

$$5\mathrm{P}\quad \left(\frac{150239953626225729846}{48615556683309804721},\ -\frac{120240529120453345949105845555}{3389712732371459185705571377 69}\right)$$

も得る．（Y 座標の符号に注意）　次の例 2.13 は P, 2P, 4P の X 座標を使って作った例である．

例 2.13 $(m_x,\ m_y,\ m_z) = \left(6,\ \dfrac{1369}{840},\ \dfrac{6655166817121}{5375193630240}\right)$

$$\Longrightarrow x = \frac{1853400388998344922950993 23}{3676920163048419500384304 0},$$

$$y = \frac{1853400388998344922950993 23}{4218556450131281530346592 0},$$

$$z = \frac{1356391649686056237391500081344928284031847001601 4843}{2203396028709098772588357954548133309906410834962560}$$

この場合

$$\sqrt{x^2+(x+y+z)} = \frac{127\cdot 4271\cdot 381650041\cdot 895304245859}{2^5\cdot 3\cdot 5\cdot 7\cdot 23\cdot 37\cdot 41\cdot 79\cdot 14321\cdot 62921\cdot 3468481}$$

$$\sqrt{x^2-(x+y+z)} = \frac{127\cdot 4271\cdot 381650041\cdot 895304245859}{2^5\cdot 3\cdot 5\cdot 7\cdot 37\cdot 41\cdot 47\cdot 79\cdot 14321\cdot 62921\cdot 3468481}$$

$$\sqrt{y^2+(x+y+z)} = \frac{127\cdot 4271\cdot 381650041\cdot 895304245859}{2^6\cdot 3\cdot 5\cdot 7\cdot 23^2\cdot 37^2\cdot 41\cdot 47^2\cdot 79\cdot 14321\cdot 62921}$$

$$\sqrt{y^2-(x+y+z)} = \frac{127\cdot 4271\cdot 381650041\cdot 895304245859}{2^6\cdot 3\cdot 5\cdot 7\cdot 23^2\cdot 37^2\cdot 41\cdot 47^2\cdot 62921\cdot 3468481}$$

$$\sqrt{z^2+(x+y+z)} = \frac{31\cdot 127\cdot 383\cdot 4271\cdot 364543\cdot 381650041\cdot 895304245859\cdot 20087744770969439}{2^7\cdot 3\cdot 5\cdot 7\cdot 23^2\cdot 37^2\cdot 41^2\cdot 47^2\cdot 79^2\cdot 14321^2\cdot 62921^2\cdot 3468481^2}$$

$$\sqrt{z^2-(x+y+z)} = \frac{127\cdot 1151\cdot 4271\cdot 381650041\cdot 895304245859\cdot 48781130986977442514689}{2^7\cdot 3\cdot 5\cdot 7\cdot 23^2\cdot 37^2\cdot 41^2\cdot 47^2\cdot 79^2\cdot 14321^2\cdot 62921^2\cdot 3468481^2}$$

□

3P, 4P, 5P の X 座標を使うともっと激しい例が作成できる.

例 2.14

$$x = \frac{61 \cdot 241 \cdot 14629 \cdot 454151 \cdot 11153809 \cdot 42769511 \cdot 2352287114951 \cdot 3341318229592841964091 \cdot 19412314690185953056521493837}{2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 41 \cdot 47 \cdot 79 \cdot 101 \cdot 179^2 \cdot 193^2 \cdot 503^2 \cdot 509 \cdot 769 \cdot 1229 \cdot 3671^2 \cdot 14321 \cdot 17539 \cdot 57259 \cdot 62921 \cdot 3468481 \cdot 4071601 \cdot 6930961}$$

$$y = \frac{113 \cdot 241 \cdot 24977 \cdot 454151 \cdot 42769511 \cdot 2753519633 \cdot 9416921777 \cdot 2352287114951 \cdot 3341318229592841964091 \cdot 19412314690185953056521493837}{2^7 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23^2 \cdot 29 \cdot 37^2 \cdot 41^2 \cdot 47^2 \cdot 79^2 \cdot 101 \cdot 179 \cdot 193 \cdot 503 \cdot 509 \cdot 769 \cdot 1229 \cdot 3671 \cdot 14321^2 \cdot 17539 \cdot 57259 \cdot 62921^2 \cdot 3468481^2 \cdot 4071601 \cdot 6930961}$$

$$z = \frac{73 \cdot 97 \cdot 181 \cdot 241 \cdot 7873 \cdot 60217 \cdot 454151 \cdot 42769511 \cdot 2352287114951 \cdot 3341318229592841964091 \cdot 1109134207785288854618461 \cdot 19412314690185953056521493837}{2^5 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 29^2 \cdot 41 \cdot 47 \cdot 79 \cdot 101^2 \cdot 179 \cdot 193 \cdot 503 \cdot 509^2 \cdot 769^2 \cdot 1229^2 \cdot 3671 \cdot 14321 \cdot 17539^2 \cdot 57259^2 \cdot 62921 \cdot 3468481 \cdot 4071601^2 \cdot 6930961^2}$$

第 3 章

合同数に関して知られていること

前章では m_x を一つ決めておいて $n=\varphi(m_x)$ を求め，$\varphi(m)=n$ となる他の m を計算した．この場合 n は合同数になると決まっているのだから m の存在は保証されるのだが，先に（平方因子を持たない）自然数 n を決めておいたとき n が合同数であるかどうかはわかるのであろうか．

$n=1,\ 2,\ 3,\ 4$ は合同数ではない．$n=5,\ 6$ は合同数である．どのような（平方因子を持たない）自然数が合同数であるかに関しては，次の驚くべき事実がある．

定理 3.1 （Tunnnel 1983）

n は平方因子をもたない自然数とし、整数 $A_n,\ B_n,\ C_n,\ D_n$ を以下で定義する．

$$\begin{aligned} A_n &= \#\{x,y,z\in\mathbb{Z}\,|\,n=2x^2+y^2+32z^2\} \\ B_n &= \#\{x,y,z\in\mathbb{Z}\,|\,n=2x^2+y^2+8z^2\} \\ C_n &= \#\{x,y,z\in\mathbb{Z}\,|\,n=8x^2+2y^2+64z^2\} \\ D_n &= \#\{x,y,z\in\mathbb{Z}\,|\,n=8x^2+2y^2+16z^2\} \end{aligned}$$

このとき n が奇数の合同数ならば $2A_n=B_n$ を、偶数の合同数ならば $2C_n=D_n$ を満たす．さらに、(弱い意味での）バーチ・スウィンナートン＝ダイアー予想が正しければ、合同数はそのような数に限る．

証明は半整数ウェイトの保型形式の空間を考えるもので，難しい． □

$n=1$ が合同数でないのは $A_1=B_1=2$ からわかる．$n=2$ が合同数でないのは $C_2=D_2=2$ からわかる．$n=5$ は合同数であり $A_5=B_5=0$ で $2A_5=B_5$ が成り立っている．