

Diophantine 方程式の整数解と一次変換

整数係数の（多変数）多項式を等号で結んだ形の方程式を、特にその整数解に注目する場合に Diophantine（ディオファントス）方程式と言います。

ここでは代表的な Diophantine 方程式である Pythagorean 方程式と Pell's 方程式についてその整数解を求めてみましょう。意外なところで線形代数の技法が活用されることになります。

1 Pythagorean 方程式の整数解

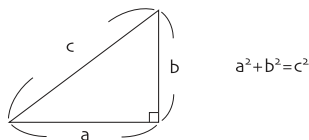
1.1 3 平方の定理

定理 1.1 直角三角形の斜辺の長さの自乗は、他の 2 辺の長さの自乗の和に等しい。

また、逆に、ある三角形の 3 辺の長さがそれぞれ a, b, c で、これらが

$$a^2 + b^2 = c^2$$

を満たすならば、その三角形は長さ c の辺を斜辺とする直角三角形である。



$3^2 + 4^2 = 5^2$ であって 3 辺が 3、4、5 の三角形が直角三角形であることはご存知の筈ですが、ここで問題です。

問題 1.2 上に挙げた 3、4、5 の組み合わせ以外で Pythagorean 方程式：

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

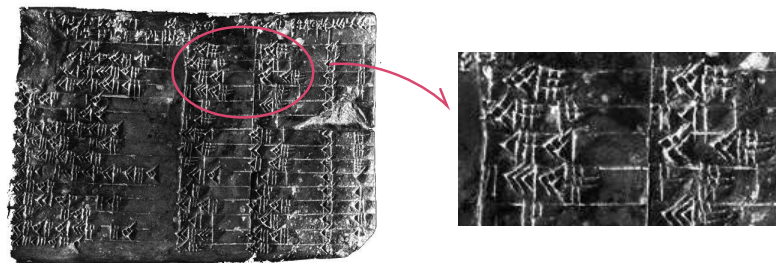
を満たす正の整数の組を他に探してみてください。

1.2 昔の人が見つけた答え

例えばこんな解があります：

$$12709^2 + 13500^2 = 18541^2$$

凄いといしか言いようのない解ですが、実はコレ、紀元前 1900-1600 年頃と推定される古代 Babylonia の遺跡から発掘された粘土板に刻まれていたんです。



ちょっと見難いですが、右の抜き出し画像を見て下さい。何やら楔形の文字が 4 段ほど確認出来ますね～これは見やすくするとこんな風（下図）になっています：



『|』が 1 を表し、『<』が 10 を表しています。何だか時刻みたいな数字が読み取れますが、そうです、60 進法なんです。

まず 1 段目に注目すると、『1;59』と『2;49』は、10 進法で言えば $1 \times 60 + 59 = 119$, $2 \times 60 + 49 = 169$ を表しています。で、こいつらは何かと云うと $169^2 - 119^2 = 14400 = 120^2$ ですから

$$119^2 + 120^2 = 169^2$$

なんですね～ もう 1 つ、4 段目も見してみましょう。これは 3; 31; 49 = $3 \times 60^2 + 31 \times 60 + 49 = 12709$, 5; 09; 01 = $5 \times 60^2 + 9 \times 60 + 1 = 18541$ であって、こちらは

$$18541^2 - 12709^2 = 182250000 = 13500^2$$

です。凄いと思いませんか？だって紀元前 1900-1600 年ですよ、3 千年以上前です。

更にこの粘土板、15 段の表が書かれていて、今見た 1 段目、4 段目以外の段にも全て同様に直角三角形の辺の長さの組み合わせが刻まれていて、詳しく見るとひとつの角が大体 30 度から 45 度までをほぼ 1 度刻みで実現しているんです。

古代 Babylonia の人たちは一体どうやってこれらの整数を求めたのでしょうか？

1.3 解の一般的な形

Pythagorean 方程式の (自明でない) 整数解 (l, m, n) があったとき、

$$l^2 + m^2 = n^2, \quad \text{すなわち} \quad \left(\frac{l}{n}\right)^2 + \left(\frac{m}{n}\right)^2 = 1$$

が成り立っていますから、 $(\frac{l}{n}, \frac{m}{n})$ は単位円周上の有理点です。逆に、単位円周上の任意の有理点 $(\frac{l}{n}, \frac{m}{n})$ に対して、 (l, m, n) は Pythagorean 方程式の 1 つの整数解になりますから、結局問題は単位円周上の有理点を見つけることです。

円周上の点 $(-1, 0)$ を通り傾きが有理数であるような直線 $y = \frac{m}{n}(x+1)$ を考えて、この直線と円周のもう 1 つの交点を求めると、直線の方程式を円周の方程式に代入して得られる 2 次方程式：

$$x^2 + \frac{m^2}{n^2}(x+1)^2 = 1, \quad \text{整理して} \quad (m^2 + n^2)x^2 + 2m^2x + m^2 - n^2 = 0$$

の左辺を因数分解して

$$(m^2 + n^2)x^2 + 2m^2x + m^2 - n^2 = (x+1)\{(m^2 + n^2)x - (n^2 - m^2)\}$$

ですから $x = \frac{n^2 - m^2}{n^2 + m^2}$ であることが分かります。このとき $y = \frac{m}{n}(x+1) = \frac{2mn}{n^2 + m^2}$ ですからこれは有理点です。

逆に、円周上の任意の有理点と $(-1, 0)$ を結ぶ直線の傾きは有理数ですから、すべての有理点がこの方法で見つかることが分かります。つまり、単位円周上の任意の有理点は $(\frac{n^2 - m^2}{n^2 + m^2}, \frac{2mn}{n^2 + m^2})$ の形をしていることが分かりました。これを Pythagorean 方程式の解に移し替えれば次の結果が得られます：

定理 1.3 Pythagorean 方程式 $x^2 + y^2 = z^2$ の正の整数解のうち最大公約数が 1 のものは、必ずある互いに素な正の整数 $m < n$ によって

$$n^2 - m^2, \quad 2mn, \quad n^2 + m^2$$

と書けます。ただし x と y はどちらかが $n^2 - m^2$ でありもう一方が $2mn$ です。

例の粘土板に残された 15 組の解を導きだすために、恐らく古代 Babylonia の人たちもこの式を知っていたであろうと推測されています。Pythagoras さん (Πυθαγόρας, ピタゴラス, c.570 – c.495 BC) はこの式だけでなく、 $2n+1$, $2n^2+2n$, $2n^2+2n+1$ と云う解の表現も知っていたようですが、厳密な証明をきちんとした形で残したのは紀元後、350 年頃に出された Euclid さんの『原論』が最初とされています。

1.4 解の一次変換

同様に考えて有理点 $(\frac{4}{5}, \frac{3}{5})$ は単位円周上にありますが、この点の極座標を $(1, \theta)$ とすると $(0 < \theta < \frac{\pi}{2})$ 、角度 θ の回転行列は

$$R_\theta = \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} \\ \frac{3}{5} & \frac{4}{5} \end{pmatrix}$$

です。この行列の成分は全て有理数ですから、 R_θ の表す一次変換で有理点を動かすと、移り先も有理点になります。例えば有理点 $(\frac{4}{5}, \frac{3}{5})$ の移り先は

$$R_\theta \begin{pmatrix} \frac{4}{5} \\ \frac{3}{5} \end{pmatrix} = \frac{1}{25} \begin{pmatrix} 4 & -3 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \frac{1}{25} \begin{pmatrix} 7 \\ 24 \end{pmatrix}$$

であり、この点も単位円周上にありますから、

$$7^2 + 24^2 = 25^2$$

が成立している筈です。

更に単位円周上の有理点 $(\frac{7}{25}, \frac{24}{25})$ を R_θ で動かしてゆくと

$$R_\theta \begin{pmatrix} \frac{7}{25} \\ \frac{24}{25} \end{pmatrix} = \frac{1}{125} \begin{pmatrix} 4 & -3 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 7 \\ 24 \end{pmatrix} = \frac{1}{125} \begin{pmatrix} -44 \\ 117 \end{pmatrix}$$

$$R_\theta \begin{pmatrix} \frac{-44}{125} \\ \frac{117}{125} \end{pmatrix} = \frac{1}{625} \begin{pmatrix} 4 & -3 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} -44 \\ 117 \end{pmatrix} = \frac{1}{625} \begin{pmatrix} -527 \\ 336 \end{pmatrix}$$

という具合に、Pythagorean 方程式の整数解が順次得られて行きます：

$$3^2 + 4^2 = 5^2 \rightarrow 7^2 + 24^2 = 25^2 \rightarrow 44^2 + 117^2 = 125^2 \rightarrow 527^2 + 336^2 = 625^2$$

一般には

$$R_\theta^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

を求めれば良いようですが、これはどうなるのでしょうか？ これによって無限個の解が得られるように思われますが、ひょっとしてある N で $R_\theta^N = E$ となったりするのでしょうか？ もしそうなら (この方法では) 有限個の解しか出てこないことになります。

これは

$$\begin{pmatrix} \cos N\theta & -\sin N\theta \\ \sin N\theta & \cos N\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \iff N\theta = 2M\pi \iff \theta = \frac{2M\pi}{N}$$

でしょうが (M は整数)、このような角度 θ で、 R_θ の各成分が有理数になるものはあるのでしょうか？ (発展演習 14 参照)

2 Pell's 方程式

次のタイプの方程式は Pell's 方程式と呼ばれています：

$$x^2 - 5y^2 = 1$$

自明な解 $(x, y) = (1, 0)$ があり、更に調べて行くと、 $5 \cdot 4^2 + 1 = 9^2$ すなわち、 $9^2 - 5 \cdot 4^2 = 1$ である事が解りました。従って $(x, y) = (9, 4)$ も整数解ですね。で、もう一個見つけたいと思う訳ですが・・・

n	1	2	3	4	5	6	7	8	9	...
n^2	1	4	9	16	25	36	49	64	<u>81</u>	
$5n^2 + 1$	6	21	46	<u>81</u>						

2.1 解の一次変換

この Pell 方程式の表す曲線は双曲線（漸近線 $x = \pm\sqrt{5}y$ は直交しません）です。従って $(1, 0)$, $(9, 4)$ が解であると言う事は、この 2 点が双曲線上にあると言うことを意味します。

対称性から点 $(9, -4)$ もこの双曲線上にあり（これも整数解です）、このようにして得られた 3 点を $(9, -4)$ から始めて

$$(9, -4) \rightarrow (1, 0) \rightarrow (9, 4)$$

と時計回りに動くような一次変換を考えましょう（右図）。

この一次変換の表現行列を M とすると、

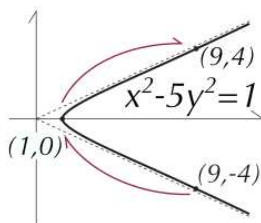
$$M \begin{pmatrix} 9 & 1 \\ -4 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 9 \\ 0 & 4 \end{pmatrix}$$

$$M = \begin{pmatrix} 1 & 9 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 9 & 1 \\ -4 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 9 \\ 0 & 4 \end{pmatrix} \frac{1}{4} \begin{pmatrix} 0 & -1 \\ 4 & 9 \end{pmatrix} = \begin{pmatrix} 9 & 20 \\ 4 & 9 \end{pmatrix}$$

となる事がわかります。

さて準備が整いました。上の図の一次変換の矢印を良く見て下さい。この先が気になりますか？ ちょっと計算してみましょう。

$$(9, -4) \rightarrow (1, 0) \rightarrow (9, 4) \rightarrow ?$$



$$M \begin{pmatrix} 9 \\ 4 \end{pmatrix} = \begin{pmatrix} 9 & 20 \\ 4 & 9 \end{pmatrix} \begin{pmatrix} 9 \\ 4 \end{pmatrix} = \begin{pmatrix} 161 \\ 72 \end{pmatrix}$$

これは

$$161^2 - 5 \cdot 72^2 = 25921 - 25920 = 1$$

ですから、Pell の方程式 $x^2 - 5y^2 = 1$ を満たしています。更にこの点を動かすと、

$$M \begin{pmatrix} 161 \\ 72 \end{pmatrix} = \begin{pmatrix} 9 & 20 \\ 4 & 9 \end{pmatrix} \begin{pmatrix} 161 \\ 72 \end{pmatrix} = \begin{pmatrix} 2889 \\ 1292 \end{pmatrix}$$

ですが、こちらも

$$2889^2 - 5 \cdot 1292^2 = 8346321 - 8346320 = 1$$

となって確かに Pell の方程式 $x^2 - 5y^2 = 1$ を満たしています。つまり

$$M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad n = 1, 2, 3, \dots$$

で得られる点は全て Pell の方程式の正の整数解になっているようです。

M の固有値は $9 \pm 4\sqrt{5}$ であり、対応する固有ベクトルは $\begin{pmatrix} \pm\sqrt{5} \\ 1 \end{pmatrix}$ です（復号同順）。これは双曲線の漸近線の方角ベクトルであることに注意します。

$$P = \begin{pmatrix} \sqrt{5} & -\sqrt{5} \\ 1 & 1 \end{pmatrix}$$

と置けば、 M は

$$P^{-1}MP = \begin{pmatrix} 9 + 4\sqrt{5} & 0 \\ 0 & 9 - 4\sqrt{5} \end{pmatrix}$$

と対角化されます。従って

$$\begin{aligned} M^n &= P \begin{pmatrix} (9 + 4\sqrt{5})^n & 0 \\ 0 & (9 - 4\sqrt{5})^n \end{pmatrix} P^{-1} \\ &= \begin{pmatrix} \sqrt{5} & -\sqrt{5} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} (9 + 4\sqrt{5})^n & 0 \\ 0 & (9 - 4\sqrt{5})^n \end{pmatrix} \frac{1}{2\sqrt{5}} \begin{pmatrix} 1 & \sqrt{5} \\ -1 & \sqrt{5} \end{pmatrix} \\ &= \frac{1}{2\sqrt{5}} \begin{pmatrix} \sqrt{5} \left\{ (9 + 4\sqrt{5})^n + (9 - 4\sqrt{5})^n \right\} & 5 \left\{ (9 + 4\sqrt{5})^n - (9 - 4\sqrt{5})^n \right\} \\ (9 + 4\sqrt{5})^n - (9 - 4\sqrt{5})^n & \sqrt{5} \left\{ (9 + 4\sqrt{5})^n + (9 - 4\sqrt{5})^n \right\} \end{pmatrix} \end{aligned}$$

$$M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2\sqrt{5}} \begin{pmatrix} \sqrt{5} \left\{ (9 + 4\sqrt{5})^n + (9 - 4\sqrt{5})^n \right\} \\ (9 + 4\sqrt{5})^n - (9 - 4\sqrt{5})^n \end{pmatrix}$$

が得られますから、任意の $n = 1, 2, \dots$ に対して

$$(x, y) = \left(\frac{1}{2} \left\{ (9 + 4\sqrt{5})^n + (9 - 4\sqrt{5})^n \right\}, \frac{1}{2\sqrt{5}} \left\{ (9 + 4\sqrt{5})^n - (9 - 4\sqrt{5})^n \right\} \right)$$

は全て問題の Pell 方程式の正の整数解になっています。

あるいは、初期値を固有ベクトルで展開する方法もあります。つまり、

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2\sqrt{5}} \left\{ \begin{pmatrix} \sqrt{5} \\ 1 \end{pmatrix} - \begin{pmatrix} -\sqrt{5} \\ 1 \end{pmatrix} \right\}$$

によれば、

$$\begin{aligned} M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \frac{1}{2\sqrt{5}} \left\{ M^n \begin{pmatrix} \sqrt{5} \\ 1 \end{pmatrix} - M^n \begin{pmatrix} -\sqrt{5} \\ 1 \end{pmatrix} \right\} \\ &= \frac{1}{2\sqrt{5}} \left\{ (9 + 4\sqrt{5})^n \begin{pmatrix} \sqrt{5} \\ 1 \end{pmatrix} - (9 - 4\sqrt{5})^n \begin{pmatrix} -\sqrt{5} \\ 1 \end{pmatrix} \right\} \\ &= \frac{1}{2\sqrt{5}} \begin{pmatrix} \sqrt{5} \left\{ (9 + 4\sqrt{5})^n + (9 - 4\sqrt{5})^n \right\} \\ (9 + 4\sqrt{5})^n - (9 - 4\sqrt{5})^n \end{pmatrix} \end{aligned}$$

ですね、こちらの方が圧倒的に早いです。

2.2 双曲回転

一般に双曲線関数：

$$\cosh \theta = \frac{e^\theta + e^{-\theta}}{2}, \quad \sinh \theta = \frac{e^\theta - e^{-\theta}}{2}$$

は関係式：

$$\cosh^2 \theta - \sinh^2 \theta = 1$$

を満たしており、従って

$$\cosh^2 \theta - 5 \left(\frac{\sinh \theta}{\sqrt{5}} \right)^2 = 1$$

ですから、

$$\begin{pmatrix} \cosh \theta \\ -\frac{\sinh \theta}{\sqrt{5}} \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} \cosh \theta \\ \frac{\sinh \theta}{\sqrt{5}} \end{pmatrix}$$

と移す一次変換の表現行列 R_θ を求めると

$$R_\theta \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cosh \theta & 1 \\ -\frac{\sinh \theta}{\sqrt{5}} & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cosh \theta \\ -\frac{\sinh \theta}{\sqrt{5}} \end{pmatrix}$$

$$R_\theta = \begin{pmatrix} \cosh \theta & \sqrt{5} \sinh \theta \\ \frac{\sinh \theta}{\sqrt{5}} & \cosh \theta \end{pmatrix}$$

です。

(x, y) が双曲線 $x^2 - 5y^2 = 1$ 上にある場合、その R_θ による像 (X, Y) についても

$$\begin{pmatrix} X \\ Y \end{pmatrix} = R_\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cosh \theta x + \sqrt{5} \sinh \theta y \\ \frac{\sinh \theta}{\sqrt{5}} x + \cosh \theta y \end{pmatrix}$$

$$\begin{aligned} X^2 - 5Y^2 &= (\cosh \theta x + \sqrt{5} \sinh \theta y)^2 - 5 \left(\frac{\sinh \theta}{\sqrt{5}} x + \cosh \theta y \right)^2 \\ &= (\cosh^2 \theta - \sinh^2 \theta) x^2 - 5(\cosh^2 \theta - \sinh^2 \theta) y^2 \\ &= (\cosh^2 \theta - \sinh^2 \theta)(x^2 - 5y^2) \\ &= 1 \end{aligned}$$

となって、像はこの双曲線上にあります。この一次変換は双曲線上の『回転』と考えることができます。先に見た行列 M は $\cosh \theta = 9, \sinh \theta = 4\sqrt{5}$ の場合であり、 $\theta = \log(9 + 4\sqrt{5})$ に対応しています。

漸近線が直交する『標準的な』双曲線 $x^2 - y^2 = 1$ 上の回転行列は

$$H_\theta = \begin{pmatrix} \cosh \theta & \sinh \theta \\ \sinh \theta & \cosh \theta \end{pmatrix}$$

です（基本演習 3）。

ちなみに斜交した漸近線をもつ双曲線 $x^2 - 5y^2 = 1$ 上の回転 R_θ は、まず y 軸方向に $\sqrt{5}$ 倍拡大して、 H_θ で回転して、 y 軸方向に $\frac{1}{\sqrt{5}}$ 倍して元に戻すことを意味します：

$$\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{5}} \end{pmatrix} H_\theta \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{5} \end{pmatrix} = \begin{pmatrix} \cosh \theta & \sinh \theta \\ \frac{\sinh \theta}{\sqrt{5}} & \frac{\cosh \theta}{\sqrt{5}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{5} \end{pmatrix} = \begin{pmatrix} \cosh \theta & \sqrt{5} \sinh \theta \\ \frac{\sinh \theta}{\sqrt{5}} & \cosh \theta \end{pmatrix} = R_\theta$$

Exercise

● Diophantine 方程式と一次変換

基本演習 1 次の Pell's 方程式の正の整数解を出来るだけたくさん見つけて下さい。

$$(1) x^2 - 3y^2 = 1 \quad (2) x^2 - 4y^2 = 1$$

基本演習 2 (a, b, c) が Pythagorean 方程式の正の整数解であるとき、これを行列

$$\begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}$$

で一次変換した点も Pythagorean 方程式の正の整数解になっていることを確認して下さい。

基本演習 3 (x, y) が $x^2 - y^2 = 1$ を満たしているとき、この点の H_θ による像も $x^2 - y^2 = 1$ を満たすことを証明して下さい。

基本演習 4 $H_{\log \frac{n}{m}}$ による点 $(1, 0)$ の像を計算することによって、Pythagorean 方程式の整数解について考えて下さい。

基本演習 5 双曲線上の回転行列 H_θ を使って、双曲線関数の『加法定理』『倍角の公式』を導いて下さい。

発展演習 6 Pell's 方程式 $x^2 - 5y^2 = 1$ の任意の正の整数解が今日見た形であることを証明して下さい。

● 整数問題

発展演習 7 (1) 方程式: $x^2 - y^2 = 3$ の整数解を全て求めてください。

(2) 方程式: $x^2 - y^2 = 3$ の有理数解を全て求めてください。

基本演習 8 (1) 任意の整数 a に対して a^2 を 4 で割った余りは 0 か 1 であることを証明して下さい。

(2) 正の整数 a, b, c が $a^2 + b^2 = c^2$ を満たすとき、 a, b が奇数で c が偶数の場合はないことを証明して下さい。

(3) 最大公約数が 1 である正の整数の組 a, b, c が $a^2 + b^2 = c^2$ を満たすとき、 a, b は一方が奇数、もう一方が偶数であることを証明して下さい。

基本演習 9 (1) 任意の整数 a に対して a^2 を 3 で割った余りは 0 か 1 であることを証明して下さい。

(2) 正の整数 a, b, c が $a^2 + b^2 = 3c^2$ を満たすと仮定すると、 a, b, c は全て 3 の倍数であることを証明して下さい。

(3) 方程式 $x^2 + y^2 = 3z^2$ は正の整数解をもたないことを証明して下さい。

発展演習 10 方程式 $2x^2 + 3y^2 = z^2$ は正の整数解をもたないことを証明して下さい。

発展演習 11 (1) あなたは次の等式を見て驚く心をもっていますか：

$$65^2 = 16^2 + 63^2 = 25^2 + 60^2 = 33^2 + 56^2 = 39^2 + 52^2.$$

(2) 上のような例を他に見つけることは出来ますか。

発展演習 12 (1) 方程式 $x^4 + y^4 = z^2$ が正の整数解をもたない事を示して下さい。

(2) 4 次の Pythagorean 方程式 $x^4 + y^4 = z^4$ が正の整数解をもたない事を示して下さい。

発展演習 13 方程式: $x^2 - y^2 - 34y = 1$ の正の整数解を全て求めてください。

発展演習 14 q を有理数とすると、 $\sin q\pi, \cos q\pi$ が共に有理数になるような角度 $0 \leq q\pi < 2\pi$ は、 $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ しかないことを示して下さい。とても難しいと思いますので、色々考えてみて下さい。

発展演習 15 楕円 $x^2 + 5y^2 = 1$ 上の有理点を双曲線 $x^2 - 5y^2 = 1$ 上の有理点に移す写像 T ：

$$T(x, y) = \left(\frac{1}{x}, \frac{y}{x} \right)$$

について、色々考えてみて下さい。

発展演習 16 (1) 円周上に有理点がある場合、無限個あることを示して下さい。

(2) 有理点が 1 つもないような円周の例を挙げて下さい。

発展演習 17 平面内の有理点を結んで出来る三角形は正三角形にならないことを示して下さい。