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

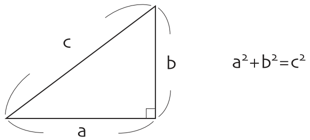
1.1　３平方の定理

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：

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

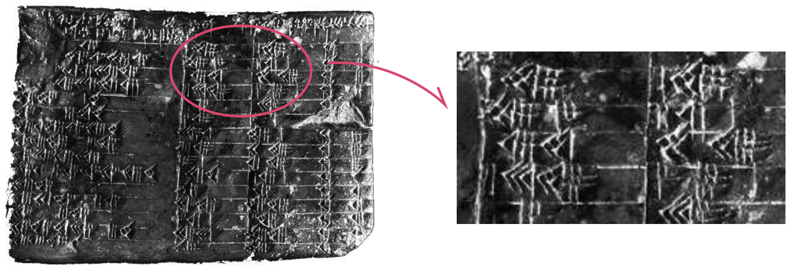
を満たす正の整数の組を他に探してみて下さい。

1.2　昔の人が見つけた答え

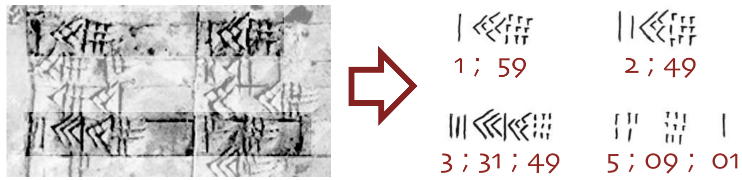
例えばこんな解があります：

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

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）になっていて：



『 | 』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 $1\times60+59=119$, $2\times60+49=169$ 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 段目も見てみましょう。これは $3;31;49=3\times60^2+31\times60+49=12709$, $5;09;01=5\times60^2+9\times60+1=18541$ 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、$\left(\frac{l}{n}, \frac{m}{n}\right)$ 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 $\left(\frac{l}{n}, \frac{m}{n}\right)$ 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

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

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 $\left(\frac{n^2-m^2}{n^2+m^2}, \frac{2mn}{n^2+m^2}\right)$ 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（$\Pi\upsilon\theta\alpha\gamma\acute{o}\rho\alpha\varsigma$、ピタゴラス、c.570 ー c.495 BC）はこの式だけでなく、$2n+1, \quad 2n^2+2n, \quad 2n^2+2n+1$ 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 $\left(\frac{4}{5}, \frac{3}{5}\right)$ は単位円周上にありますが、この点の極座標を $\langle 1, \theta \rangle$ 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 $\left(\frac{4}{5}, \frac{3}{5}\right)$ 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 $\left(\frac{7}{25}, \frac{24}{25}\right)$ 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：

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

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なと思う訳ですが・・・

n	1	2	3	4	5	6	7	8	9	$\cdots$
n^2	1	4	9	16	25	36	49	64	$\underline{81}$	
$5n^2 + 1$	6	21	46	$\underline{81}$						

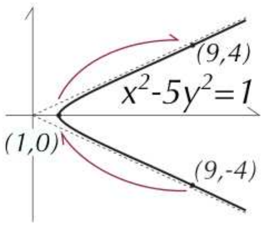
2.1　解の一次変換

　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 $(1, 0)$, $(9, 4)$ が解であると云う事は、この２点が双曲線上にあると云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

$$(9, -4) \quad \to \quad (1, 0) \quad \to \quad (9, 4)$$

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せんか？　ちょっと計算してみましょう。

$$(9, -4) \quad \to \quad (1, 0) \quad \to \quad (9, 4) \quad \to \quad ?$$

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

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

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

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、対応する固有ヴェクターは $\begin{pmatrix} \pm\sqrt{5} \\ 1 \end{pmatrix}$ です（復号同順）。これは双曲線の漸近線の方向ヴェクター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

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

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、初期値を固有ヴェクター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、

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

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：

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

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、

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

と移す一次変換の表現行列 R_θ を求めると

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

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

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

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

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

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るでしょう。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) $x^2 - 3y^2 = 1$　　(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 を有理数とするとき、$\sin q\pi, \cos q\pi$ 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、色々と考えてみて下さい。

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。

Exercise 解答例

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

(1) まず正とは限らず全ての整数の中で解を探すと、$(x, y) = (1, 0)$ は自明な解です。また、$(x, y) = (2, 1)$ が解であることもすぐに分かるでしょう。このときやはり $(x, y) = (2, -1)$ も解であることに注意します。
そこで

$$(2, -1) \quad \to \quad (1, 0) \quad \to \quad (2, 1)$$

と点を移す一次変換の表現行列を M とすれば、

$$\begin{aligned} M \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \\ M &= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \end{aligned}$$

となります。この一次変換によって点 $(2, 1)$ が移る先を計算すると

$$M \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix}$$

であり、

$$7^2 - 3 \cdot 4^2 = 49 - 3 \cdot 16 = 49 - 48 = 1$$

となっていてこれは問題の方程式の正の整数解です。同様に更なる移り先を計算してゆけば

$$(26, 15), \quad (97, 56), \quad (362, 209)$$

などが得られます。

(2) 方程式を変形すると

$$x^2 = (2y)^2 + 1$$

なので正の整数解 (x, y) については必ず $x \geq 2y + 1$ が成り立ちます。このとき

$$x^2 \geq (2y + 1)^2 = (2y)^2 + 4y + 1$$

ですから、$x^2 = (2y)^2 + 1$ であるためには $y = 0$ しかあり得ません。従って正の整数解は存在しません。 □

基本演習 2 (a, b, c) が Pythagorean 方程式の正の整数解であるとき、これを今日見た行列 $\begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}$ 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。

行列：

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

の表現する３次元空間内の一次変換による点 (a, b, c) の移り先は

$$\begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a + 2b + 2c \\ 2a + b + 2c \\ 2a + 2b + 3c \end{pmatrix}$$

ですが、計算すると

$$\begin{aligned} &(a + 2b + 2c)^2 + (2a + b + 2c)^2 \\ &= 5a^2 + 5b^2 + 8c^2 + 8ab + 12bc + 12ca \\ &= (2a)^2 + (2b)^2 + (3c)^2 + 2 \cdot 2a \cdot 2b + 2 \cdot 2b \cdot 3c + 2 \cdot 3c \cdot 2a + a^2 + b^2 - c^2 \\ &= (2a + 2b + 3c)^2 + a^2 + b^2 - c^2 \end{aligned}$$

となっており、もしも $a^2 + b^2 = c^2$ が成り立っているならば、点 (a, b, c) の移り先である点 $(a + 2b + 2c, 2a + b + 2c, 2a + 2b + 3c)$ も $(a + 2b + 2c)^2 + (2a + b + 2c)^2 = (2a + 2b + 3c)^2$ を満たすことになります。 □

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。

(x, y) が $x^2 - y^2 = 1$ をみたすとき、

$$H_\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cosh\theta x + \sinh\theta y \\ \sinh\theta x + \cosh\theta y \end{pmatrix}$$

であって、$\cosh^2\theta - \sinh^2\theta = 1$ に注意すれば

$$(\cosh\theta x + \sinh\theta y)^2 - (\sinh\theta x + \cosh\theta y)^2 = (\cosh^2\theta - \sinh^2\theta)x^2 - (\cosh^2\theta - \sinh^2\theta)y^2 = 1$$

となり、確かに変換後の点も $x^2 - y^2 = 1$ 上にあります。 □

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。

$$\cosh\log\frac{n}{m}=\frac{\frac{n}{m}+\frac{m}{n}}{2}=\frac{n^2+m^2}{2mn},\quad \sinh\log\frac{n}{m}=\frac{\frac{n}{m}-\frac{m}{n}}{2}=\frac{n^2-m^2}{2mn}$$

$$H_{\log\frac{n}{m}}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}\frac{n^2+m^2}{2mn}\\\frac{n^2-m^2}{2mn}\end{pmatrix}$$

従って点 $\left(\frac{n^2+m^2}{2mn},\frac{n^2-m^2}{2mn}\right)$ は双曲線 $x^2-y^2=1$ 上にあり、

$$(n^2+m^2)^2-(n^2-m^2)^2=(2mn)^2$$

ですが、これは点 $(1,0)$ を有理数の対数であるような『角』で『回転』すれば、Pythagorean 方程式の任意の（既約な）解が出てくることを意味しています。 □

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。

$$\begin{aligned}&\begin{pmatrix}\cosh(\alpha+\beta) & \sinh(\alpha+\beta)\\ \sinh(\alpha+\beta) & \cosh(\alpha+\beta)\end{pmatrix}\\ &=\begin{pmatrix}\cosh\alpha & \sinh\alpha\\ \sinh\alpha & \cosh\alpha\end{pmatrix}\begin{pmatrix}\cosh\beta & \sinh\beta\\ \sinh\beta & \cosh\beta\end{pmatrix}\\ &=\begin{pmatrix}\cosh\alpha\cosh\beta+\sinh\alpha\sinh\beta & \cosh\alpha\sinh\beta+\sinh\alpha\cosh\beta\\ \cosh\alpha\sinh\beta+\sinh\alpha\cosh\beta & \cosh\alpha\cosh\beta+\sinh\alpha\sinh\beta\end{pmatrix}\end{aligned}$$

から、

$$\cosh(\alpha+\beta)=\cosh\alpha\cosh\beta+\sinh\alpha\sinh\beta$$
$$\sinh(\alpha+\beta)=\cosh\alpha\sinh\beta+\sinh\alpha\cosh\beta$$

であり、特に、

$$\cosh 2\alpha=\cosh^2\alpha+\sinh^2\alpha$$
$$\sinh 2\alpha=2\cosh\alpha\sinh\alpha$$

です。 □

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。

まず第一に、問題の Pell's 方程式の２つの非負整数解 $(a,b),(c,d)$ があって $a\le c$ であれば、$b\le d$ も成り立つことを注意しておきます（等号は $a=c,b=d$ のときのみ成り立ちます）。この意味で特別な記号：

$$\begin{pmatrix}a\\b\end{pmatrix}\le\begin{pmatrix}c\\d\end{pmatrix}$$

を使うことにします。また件の一次変換の表現行列 M は、

$$M=\begin{pmatrix}9&4\\4&20\end{pmatrix},\quad M\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}9x+4y\\4x+20y\end{pmatrix}$$

ですから、非負整数解 $(a,b),(c,d)$ に対して

$$\begin{pmatrix}a\\b\end{pmatrix}\le\begin{pmatrix}c\\d\end{pmatrix}\Leftrightarrow M\begin{pmatrix}a\\b\end{pmatrix}\le M\begin{pmatrix}c\\d\end{pmatrix}$$

となっています。そこで

$$\begin{pmatrix}x_n\\y_n\end{pmatrix}=M^n\begin{pmatrix}1\\0\end{pmatrix}$$

と置けば、数列 $\{x_n\}$ は真に単調増大列です。

従って、問題の Pell's 方程式の任意の正の整数解 $(x,y)=(a,b)$ に対して必ず

$$\begin{pmatrix}x_n\\y_n\end{pmatrix}\le\begin{pmatrix}a\\b\end{pmatrix}<\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix}$$

であるような非負整数 n がただ１つ存在します。また、

$$\begin{pmatrix}a_1\\b_1\end{pmatrix}=M^{-1}\begin{pmatrix}a\\b\end{pmatrix}$$

と置けば、$(x,y)=(a_1,b_1)$ も同じ Pell's 方程式の整数解であって

$$M^{-1}\begin{pmatrix}x_n\\y_n\end{pmatrix}\le M^{-1}\begin{pmatrix}a\\b\end{pmatrix}<M^{-1}\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix},\quad \text{即ち}\quad \begin{pmatrix}x_{n-1}\\y_{n-1}\end{pmatrix}\le\begin{pmatrix}a_1\\b_1\end{pmatrix}<\begin{pmatrix}x_n\\y_n\end{pmatrix}$$

が成り立ちますから、

$$\begin{pmatrix}a_j\\b_j\end{pmatrix}=M^{-j}\begin{pmatrix}a\\b\end{pmatrix}$$

と置いて同じ議論を繰り返せば

$$M^{-n}\begin{pmatrix}x_n\\y_n\end{pmatrix}\le M^{-n}\begin{pmatrix}a\\b\end{pmatrix}<M^{-n}\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix},\quad \text{即ち}\quad \begin{pmatrix}1\\0\end{pmatrix}\le\begin{pmatrix}a_n\\b_n\end{pmatrix}<\begin{pmatrix}9\\4\end{pmatrix}$$

が成り立ちます。しかし講義中に見たように、$1<a_n<9$ を満たす正の整数解 (a_n,b_n) は存在しませんから、自動的に $\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}a_n\\b_n\end{pmatrix}$ であることが分かります。

従って以上から
$$\begin{pmatrix} a \\ b \end{pmatrix} = M^n \begin{pmatrix} a_n \\ b_n \end{pmatrix} = M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
の形に書けることが分かりました。 □

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。

(1) $(x-y)(x+y) = x^2 - y^2 = 3$ ですから、$(x, y) = (\pm 2, \pm 1)$ の場合しかありません。

(2) $(2, 1)$ を通り傾きが有理数 Q である直線：
$$y - 1 = Q(x - 2)$$
と双曲線 $x^2 - y^2 = 3$ の交点を求めると、
$$\begin{aligned} x^2 - \{Q(x-2)+1\}^2 &= 3 \\ (x-2+2)^2 - Q^2(x-2)^2 - 2Q(x-2) &= 4 \\ (1-Q^2)(x-2)^2 + (4-2Q)(x-2) &= 0 \\ (x-2)\{(1-Q^2)(x-2) + 4 - 2Q\} &= 0 \\ (x-2)\left\{(1-Q^2)x + 2Q^2 - 2Q + 2\right\} &= 0 \end{aligned}$$
ですから、$Q \neq \pm 1$ であれば $(2, 1)$ 以外の交点 $\left(\frac{2Q^2-2Q+2}{Q^2-1}, \frac{-Q^2+4Q-1}{Q^2-1}\right)$ が得られます。これは問題の方程式の有理解になっています。

逆に、問題の方程式の有理解のうち $(2, \pm 1)$ 以外のものを１つとったとき、この有理点と点 $(2, 1)$ を結ぶ直線は傾きが有理数であり、今求めたものの中に含まれていることが分かりますから、結局、問題の方程式の有理数解は
$$(2, \pm 1), \qquad \left(\frac{2Q^2-2Q+2}{Q^2-1}, \frac{-Q^2+4Q-1}{Q^2-1}\right) \quad (Q \text{ は有理数})$$
で全てです（ただし、点 $(2, 1)$ は $Q = 2$ の場合で右のものにも含まれています）。 □

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。

(1) a が偶数か奇数かによって場合分けして考えます。

【$a = 2k$ のとき】このとき $a^2 = (2k)^2 = 4k^2$ ですから４で割った余りは０です。

【$a = 2k+1$ のとき】このときは $a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ ですから、４で割った余りは１です。

以上から題意は証明されました。

(2) a, b が奇数の場合、(1) の結果から a^2, b^2 共に４で割った余りは１となりますから、左辺を４で割った余りは２です。しかし c が偶数の場合、右辺は４の倍数となり矛盾します。従ってそのような場合はありません。

(3) (2) の結果から、a, b の少なくとも一方は偶数です。もしも両方が偶数であれば c も偶数でなければなりませんが、a, b, c の最大公約数が１であるとするとこれは矛盾します。従って必ず一方は偶数、もう一方は奇数でなければなりません。 □

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。

(1) a を３で割ったときの余りによって場合分けして考えます。
【$a = 3k$ のとき】このとき $a^2 = 9k^2$ であり３で割った余りは０です。
【$a = 3k+1$ のとき】このときは $a^2 = 9k^2 + 6k + 1$ ですから、３で割った余りは１です。
【$a = 3k+2$ のとき】このときも $a^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$ ですから、３で割った余りは１です。
以上で題意は示されました。

(2) 正の整数 a, b, c が $a^2 + b^2 = 3c^2$ を満たすと仮定します。すると $a^2 + b^2$ は３の倍数ですから、(1) の結果より a, b は共に３の倍数でなければなりません。するとこのとき左辺は９の倍数ですから c^2 が３の倍数であることになり、従って c も３の倍数です。

(3) 正の整数解 $(x, y, z) = (a, b, c)$ が存在したとします。すると (2) からそれらは全て３の倍数ですから正の整数 p, q, r によって $a = 3p, b = 3q, c = 3r$ と置けます。すると
$$\begin{aligned} (3p)^2 + (3q)^2 &= 3(3r)^2 \\ p^2 + q^2 &= 3r^2 \end{aligned}$$
となり、$(x, y, z) = (p, q, r)$ も正の整数解であることが分かります。
この議論は何度でも繰り返すことが出来、その度により小さな正の整数解が作り出される事になりますが、正の整数は１より大きいのでこの操作は現実には有限回でストップする筈です。これは矛盾ですから正の整数解は存在しないことが分かります。 □

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。

問題の方程式が整数解 $(x,y,z)=(a,b,c)$ をもてば、$(|a|,|b|,|c|)$ は非負整数解になります。また、c が 0 になる場合は $a=b=c=0$ しかあり得ませんし、a,b のいずれかが 0 である場合も 2 あるいは 3 が平方数になってしまいますから、結局のところ正の整数解が存在しないことさえ示せば十分です。

また、正の整数解 $(x,y,z)=(a,b,c)$ があって、a,b,c が 1 でない公約数 d をもつ場合、$\frac{a}{d},\frac{b}{d},\frac{c}{d}$ もまた正の整数解になりますから、結局、最大公約数が 1 の場合に証明すれば十分であることも分かります。

$(x,y,z)=(a,b,c)$ は問題の方程式の正の整数解が存在して、$\mathrm{GCD}(a,b,c)=1$ とします。このとき $2a^2+3b^2=c^2$ の両辺を 3 で割った余りを考えると、左辺の余りは 2 か 0 であり、右辺の余りは 1 か 0 ですので、両辺とも余りは 0 でなければならず、それは a,c が共に 3 の倍数である場合です。このとき仮に $a=3p,c=3r$ と置けば

$$2(3p)^2+3b^2=(3r)^2$$
$$6p^2+b^2=3r^2$$

となりますから、b^2、ひいては b も 3 の倍数でなければなりませんがそうすると $\mathrm{GCD}(a,b,c)\neq 1$ となってしまいます。これは矛盾ですから結局正の整数解は存在しないことが分かります。　□

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。

まず (1) の式を詳しく調べてみましょう。$65=5\cdot 13$ であることに注目します。

$$3^2+4^2=5^2,\quad 5^2+12^2=13^2$$

でしたから、左を 13^2 倍、右を 5^2 倍したものは

$$39^2+52^2=65^2,\quad 25^2+60^2=65^2$$

となります。また、

$$65=1^2+8^2=4^2+7^2$$

でもあるので、$(m^2-n^2,2mn,m^2+n^2)$ 型の Pythagorean 方程式の正整数解で $m^2+n^2=65$ のものが２組あります：

$(m,n)=(8,1)$ の場合：　$m^2-n^2=64-1=63,\quad 2mn=16,\quad m^2+n^2=65,$
$63^2+16^2=65^2$

$(m,n)=(7,4)$ の場合：　$m^2-n^2=49-16=33,\quad 2mn=56,\quad m^2+n^2=65,$
$33^2+56^2=65^2$

他にこのような例がないか考えると、ポイントは 65 が２通りの平方和で書けていることですから、まずそのような数を探してみます。それは沢山あります。小さいものでは

$$25=5^2+0^2=3^2+4^2,\quad 50=5^2+5^2=7^2+1^2$$

などがありますが、どちらも芳しくありません。0 は使いたくないですし、$m=n$ のケースも駄目だからです。

$125=10^2+5^2=11^2+2^2$ について考えてみると、$(m,n)=(10,5),(11,2)$ から

$$75^2+100^2=117^2+44^2=125^2$$

です。
一方 $125=5^3$ なので $3^2+4^2=5^2$ を 25^2 倍しても $75^2+100^2=125^2$ となって同じものになってしまいます。
それでも $7^2+24^2=25^2$ の 5^2 倍から $35^2+120^2=125^2$ が得られますからこれで３つです。

他に $962=11^2+29^2=1^2+31^2$ を基に調べてみると同様にして

$$962^2=720^2+638^2=960^2+62^2=370^2+888^2=910^2+312^2$$

が分かります。　□

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。

(1) が成り立てば (2) も成り立つことは自明です。

(1) 問題の方程式が正の整数解をもつと仮定します。このときそのような解の中で z に相当するものが最小のものがある筈ですから、そのような解の１つを $(x,y,z)=(a,b,c)$ とします。
証明の方針としては、この解を基にすれば別の正の整数解 (p,q,r) で $r<c$ であるものが作れてしまい、矛盾すると云う方向で行きます。

いま $a^4+b^4=c^2$ ですから、4 で割った余りを考えれば a,b が共に奇数と云う事はあり得ません。更に a,b が共に偶数である場合は c も偶数であり、$a=2a_1,b=2b_1,c=2c_1$ と置けば

$$(2a_1)^4+(2b_1)^4=(2c_1)^2$$
$$4a_1^4+4b_1^4=c_1^2$$

となり、c_1 も偶数ですから $c_1=2c_2$ と置いて

$$4a_1^4+4b_1^4=4c_2^2$$

$$a_1^4 + b_1^4 = c_2^2$$

が得られ、元の方程式の正の整数解 (a_1, b_1, c_2) で、$c_2 < c$ なるものが作れてしまい矛盾します。従って a, b が共に偶数であることはありません。

同様な議論によって a, b が 1 でない公約数をもつ場合も矛盾に到達しますので、a, b は一方が奇数、他方が偶数であって $\mathrm{GCD}(a, b) = 1$ （当然ですが $\mathrm{GCD}(a, b, c) = 1$）であることが分かります。ここでは a が偶数であるとして話を進めます（これで一般性を失いません）。

このとき (a^2, b^2, c) は Pythagorean 方程式を満たしますから

$$a^2 = 2mn, \quad b^2 = m^2 - n^2, \quad c = m^2 + n^2$$

なる正の整数 m, n が存在します。特にこのとき $\mathrm{GCD}(m, n) = 1$ でもあります（そうでないなら $\mathrm{GCD}(a, b, c) = 1$ に反する事になります）。

また、$a^2 = 2mn$ によれば a は偶数ですから右辺も 4 で割り切れねばならず、a, b のいずれか一方は偶数です。しかし、もしも m が偶数で n が奇数であれば、$b^2 = m^2 - n^2$ は 4 で割って 3 余る事になりますが、これはあり得ませんので m は奇数、n が偶数であることが分かりますので $n = 2v$ と置くことにします。すると

$$a^2 = 4mv$$

であって、$\mathrm{GCD}(m, v) = 1$ ですから、m, v は共に平方数でなければなりません。そこで $m = r^2, v = u^2$ と置くと

$$\begin{aligned} b^2 &= m^2 - n^2 \\ &= (r^2)^2 - (2u^2)^2 \\ (2u^2)^2 + b^2 &= (r^2)^2 \end{aligned}$$

となり、$(2u^2, b^2, r^2)$ は Pythagorean 方程式の正の整数解であって $\mathrm{GCD}(2u^2, b^2, r^2) = 1$ ですから

$$2u^2 = 2\alpha\beta, \quad b^2 = \alpha^2 - \beta^2, \quad r^2 = \alpha^2 + \beta^2$$

となる互いに素な正の整数 α, β が存在します。ここで第１式から $u^2 = \alpha\beta$ なので α, β は共に平方数でなければなりませんので $\alpha = p^2, \beta = q^2$ と置けば第３式から

$$r^2 = p^4 + q^4$$

が成り立っていることが分かり、(p, q, r) は問題の方程式の正の整数解です。ところが

$$r \le w^2 = m \le m^2 < m^2 + n^2 = c$$

によれば $r < c$ ですから最初に指摘した通りの解が作れてしまったことになります。これは矛盾ですから以上により正の整数解は存在しません。 □

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。

問題を次のように変形してみましょう：

$$Q(n) = n^2 + 34n + 1$$

が平方数となるような正の整数 n を全て求めてください。

$n = 1, 5$ で平方数であることはすぐに分かります：

$$Q(1) = 36 = 6^2, \qquad Q(5) = 196 = 14^2$$

まず

$$\begin{aligned} (n+17)^2 &= n^2 + 34n + 289 = Q(n) + 288 > Q(n) \\ (n+16)^2 &= n^2 + 32n + 256 = Q(n) - 2n + 255 \end{aligned}$$

ですから、$n \ge 128$ のときは $Q(n)$ は平方数にはなりません。また、$n \le 127$ であれば $Q(n) < (n+16)^2$ が成り立っており、

$$(n+15)^2 = n^2 + 30n + 225 = Q(n) - 4n + 224$$

によれば $57 \le n \le 127$ の範囲では

$$(n+15)^2 < Q(n) < (n+16)^2$$

となって平方数ではあり得ません。

$n = 56$ の場合は

$$71^2 = Q(56)$$

ですから、平方数です。

更に $n \le 55$ においては $Q(n) < (n+15)^2$ であって、

$$(n+14)^2 = n^2 + 28n + 196 = Q(n) - 6n + 195$$

に注意すれば $33 \le n \le 55$ でも平方数ではあり得ません。

また、$n \le 32$ で $Q(n) < (n+14)^2$ なので

$$(n+13)^2 = n^2 + 26n + 169 = Q(n) - 8n + 168$$

と合わせて、$22 \le n \le 32$ でも平方数ではありません。

$n = 21$ のときは

$$34^2 = Q(21)$$

ですから平方数です。

全く同様にして

$$\begin{aligned} (n+12)^2 < Q(n) < (n+13)^2 &\qquad 15 \le n \le 20 \\ (n+11)^2 < Q(n) < (n+12)^2 &\qquad 11 \le n \le 14 \\ 21^2 = Q(10)& \\ (n+10)^2 < Q(n) < (n+11)^2 &\qquad n = 8, 9 \end{aligned}$$

$$(n+9)^2 < Q(n) < (n+10)^2 \qquad n = 6, 7$$

であって、また $Q(2), Q(3), Q(4)$ は全て平方数ではないので、

$$Q(1),\ Q(5),\ Q(10),\ Q(21),\ Q(56)$$

以外の $Q(n)$ は平方数ではありません。

以上から元の問題の正の整数解は

$$(x, y) = (1, 6),\ (5, 14),\ (10, 21),\ (21, 34),\ (56, 71)$$

で全てです。

【別解】$y + 17 = Y$ と置けば、

$$\begin{aligned} x^2 - y^2 - 34y &= 1 \\ x^2 - (y+17)^2 + 288 &= 0 \\ (y+17)^2 - x^2 &= 288 \\ Y^2 - x^2 &= 2^5 \cdot 3^2 \\ (Y+x)(Y-x) &= 2^5 \cdot 3^2 \end{aligned}$$

ですから、

$$\begin{cases} Y + x = 2^l 3^m \\ Y - x = 2^{5-l} 3^{2-m} \end{cases}$$

が $Y > 17, x > 0$ であるような整数解をもつ場合を考えます。一般に連立方程式の解は

$$2x = 2^l 3^m - 2^{5-l} 3^{2-m}, \quad 2Y = 2^l 3^m + 2^{5-l} 3^{2-m}$$

ですから、$l = 1, 2, 3, 4$ しかあり得ません。それぞれ見ていきましょう。

<u>$l = 1$ の場合</u>

$$x = 3^m - 8 \cdot 3^{2-m}, \quad Y = 3^m + 8 \cdot 2^{2-m}$$

ですから、$m = 0, 1$ のときは $x < 0$ ですから解はありません。$m = 2$ のときは

$$x = 9 - 8 = 1, Y = 9 + 8 = 17$$

となってやはり解はありません。

<u>$l = 2$ の場合</u>

$$x = 2 \cdot 3^m - 4 \cdot 3^{2-m}, \quad Y = 4 \cdot 3^{2-m} + 2 \cdot 3$$

ですから、$m = 0, 1$ のときは解はありません。$m = 2$ のときは

$$x = 18 - 4 = 14, \quad Y = 4 + 18 = 22, \quad y = 5$$

となって解 $(14, 5)$ が得られます。

<u>$l = 3$ の場合</u>

$$x = 4 \cdot 3^m - 2 \cdot 3^{2-m}, \quad Y = 2 \cdot 3^{2-m} + 4 \cdot 3^m$$

ですから、$m = 0$ のときは解はありません。$m = 1$ のときは

$$x = 12 - 6 = 6, \quad Y = 6 + 12 = 18, \quad y = 1$$

となって解 $(6, 1)$ が得られます。

$m = 2$ のときは

$$x = 36 - 2 = 34, \quad Y = 2 + 36 = 38, \quad y = 21$$

となって解 $(34, 21)$ が得られます。

<u>$l = 4$ の場合</u>

$$x = 8 \cdot 3^m - 3^{2-m}, \quad Y = 3^{2-m} + 8 \cdot 3^m$$

ですから、$m = 0$ のときは解はありません。$m = 1$ のときは

$$24 - 3 = 21, \quad Y = 3 + 24 = 27, \quad y = 10$$

から解 $(21, 10)$ が得られます。$m = 2$ のときは

$$x = 72 - 1 = 71, \quad Y = 1 + 72 = 73, \quad y = 56$$

となって解 $(71, 56)$ が得られます。

以上から問題の正の整数解は

$$(x, y) = (6, 1),\ (14, 5),\ (21, 10),\ (34, 21),\ (71, 56)$$

で全てです。 □

発展演習 14 q を有理数とするとき、$\sin q\pi, \cos q\pi$ 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、色々と考えてみて下さい。

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。

まあ、いろいろと。