有理数と、円と楕円と双曲線

小川 裕之　(大阪大学大学院 理学研究科)[†]

§1　序

今日は, 図形における有理数についてお話します. 図形といっても, 円, 楕円, 双曲線, 平面に描かれたわりと単純な図形です. 「あれ? 放物線は?」と思った方は, とても鋭い感性を持っていると思います. 円, 楕円, 放物線, 双曲線は, 円錐を平面で切った断面に現れる曲線で, **円錐曲線** と呼ばれています.

§2　図形を表す方程式

2.1　座標平面　　平面に描かれた図形を表す方法はいくつもあります. 例えば直線ならば, ある点と直線の延びていく向きを指定する方法, 異なる 2 点を指定する方法があります. 円ならば, 中心と半径を指定する方法がすぐに思いつきます. でも, 三角形の外接円, 内接円を思い出せば, 円周の上の 3 つの点を指定する方法や, 3 つの直線に接する円と言った指定の仕方もあります. 平面図形の様々な性質, 特徴に従って, 様々な方法で図形を定めることも興味深いものはありますが, 今日は, 数とのかかわりを見るために, 座標平面における方程式を考えることにします. 横方向の数直線を $\boldsymbol{x}$**-軸**, 縦方向の数直線を $\boldsymbol{y}$**-軸**, それらの交点を **原点** $\boldsymbol{O}$ とする. 平面上の点に対して x-軸方向の位置と y-軸方向の位置を表す 2 つの実数の組をその点の **座標** といい, 座標を定めた平面を **座標平面** といいます. 座標平面上で図形を指定する一般的な手段は, その図形を構成する点の座標 (x,y) の x と y の満たす方程式を与えることです. 直線ならば, 傾きと y-切片を与えた $y=a\,x+b$ という一次式で定めることができます. 異なる 2 点 (p_1,q_1), (p_2,q_2) を通る直線上の点 (x,y) は, 比例関係 $(x-p_1):(y-q_1)=(p_2-p_1):(q_2-q_1)$ が成り立ちますから, $(q_2-q_1)(x-p_1)=(p_2-p_1)(y-q_1)$ という方程式を満たします. いずれにせよ直線は一次方程式 $\boldsymbol{p\,x+q\,y=r}$ で表せます. この形の便利なところは, 直線 $p\,x+q\,y=r$ と垂直に交わる直線が $q\,x-p\,y=r'$ と表せることと, y-軸に平行な直線も表せることです.

2.2　円を表す方程式　　円を表すには, 中心と半径を指定することになります. 中心の座標が (a,b) で半径が r の円は, $(x-a)^2+(y-b)^2=r^2$ で表せます. これが **円を表す方程式** です. 原点を中心とし半径 1 の円を **単位円** といい, $x^2+y^2=1$ で表されます. 円に関わる用語として半径はとても重要ですが, 方程式としては二乗の形であることに重要性はありませんから, 円を表す方程式としては $\boldsymbol{(x-a)^2+(y-b)^2=c}$ **(**$\boldsymbol{c}$ **は正の実数)** とすれば十分です. 両辺を c で割って $p=1/c$ とおいて $p\,(x-a)^2+p\,(y-b)^2=1$ と表すこともできます.

2.3　楕円を表す方程式　　楕円は, 円をある向きに拡げたり, 押しつぶしたりしたものです. 単位円を x-軸方向に 2 倍に拡げた図形を考えましょう. このとき, 点 (x,y) が点 $(2x,y)$ に動くことになり, 単位円 $x^2+y^2=1$ の点 (x,y) を $(2x,y)$ に動かしたときの $2x$ と y の満たす方程式を作ることになります. 少しややこしいので, 動いた後の点を (X,Y) としましょう. $X=2x$, $Y=y$ なので, $x=X/2$, $y=Y$ です. $x^2+y^2=1$ に代入すると $(X/2)^2+Y^2=1$ となります. X と Y の満たす方程式 $(X/2)^2+Y^2=1$ が, 単位円を x-軸方向に 2 倍に拡げた楕円を表す方程式です. x-軸方向を 2 倍に拡げるだけでなく, さらに y-軸方向を $1/3$ に縮めてみましょう. (x,y) を $(X,Y)=(2x,\,y/3)$ に動かすことになります. 先ほどと同様にして $(X/2)^2+(3Y)^2=1$ となります. 単位円を x-軸方向に u 倍, y-軸方向を v 倍した楕円を表す方程式は $x^2/u^2+y^2/v^2=1$ となります. 拡げたりつぶしたりする方向は, 横向き (x-軸方向) や縦向き (y-軸方向) だけでなく, 斜めでもかまいません. このことをどのように考えればいいでしょう. 座標平面に楕円が描かれているとしましょう. 楕円の中心の座標を (a,b) とします. 楕円の長軸 (楕円の一番伸びている向きの直線) を表す方程式を $p\,(x-a)+q\,(y-b)=0$ とおくと, 楕円の中心で長軸に垂直に交わる直線は $q\,(x-a)-p\,(y-b)=0$ で表わされます. そもそも平面に座標を定めるときに便宜上, 原点, 横方向, 縦方向を決めましたが, 原点として平面上のどの点を選んでも, 横向きとしてどの向きを選んでもかまいません. 例えば, 隣の人のノートに書いた座標を横から除きこむと, 原点は何か遠くにありますし, x-軸が横向きとも y-軸が縦向きとも限りません. ただひとつ, x-軸と y-軸が垂直に交わっていることだけです. 今考えている楕円も, 隣の人のノートでは, 中心が原点で, 長軸が x-軸方向になるように描いてあったかもしれません. 隣の人の座標と区別するために, 隣の人の座標平面は X, Y で表わされていたとします. すると, 自分の座標平面の座標 x, y との関係は, $X=s\,(x-a)+t\,(y-b)$, $Y=t\,(x-a)-s\,(y-b)$ $((s,t)\neq(0,0))$ で表わされます. ここで (a,b) はその楕円の中心を自分の座標平面において見たときの座標です. 隣の人の座標での楕円の方程式 $X^2/u^2+Y^2/v^2=1$ に $X=s\,(x-a)+t\,(y-b)$, $Y=t\,(x-a)-s\,(y-b)$ を代入すれば $p\,(x-a)^2+q\,(x-a)(y-b)+r\,(y-b)^2=1$, ただし $p=s^2/u^2+t^2/v^2$, $q=2st(1/u^2-1/v^2)$, $r=s^2/v^2+t^2/u^2$ です. このとき, $q^2-4pr=-4((s^2+t^2)/uv)^2$ なので, $q^2-4pr<0$ を満たします. こうして得られた方程式 $\boldsymbol{p\,(x-a)^2+q\,(x-a)(y-b)+r\,(y-b)^2=1}$ **(ただし** $\boldsymbol{q^2-4pr<0,\ p>0,\ r>0}$**)** が, **楕円を表す方程式** です.

2.4　双曲線を表す方程式　　楕円のときと同じようにして双曲線について考えてみましょう. 双曲線で思い出すのは, 反比例 $y=1/x$ のグラフです. 反比例 $y=1/x$ のグラフは, 第 1 象限と第 3 象限に描かれ, 原点に関して対

[†] 〒 560-0043　大阪府豊中市待兼山町 1-1　　ogawa@math.sci.osaka-u.ac.jp
2018 年 10 月 31 日　　於 奈良県立 奈良高等学校

称で, 原点から離れるに従ってグラフは x-軸か y-軸にどんどん近づいていきます. x-軸と y-軸を双曲線 $y=1/x$ の **漸近線** といいます. 双曲線の定義の仕方はいろいろありますが, 楕円のときのように, 隣の人のノートの座標平面に描かれた反比例のグラフを自分の座標平面の座標であらわすことを考えてみましょう. 今度はさらに, 隣の人のノートを少し斜めに見たとしましょう. 隣の人の X-軸や Y-軸は, 1 点で交わる 2 つの直線ですが, 斜めに見たために垂直に交わっているようには見えないこともあります. 隣の人の座標 X, Y と自分の座標 x, y との関係は $X=s\,(x-a)+t\,(y-b)$, $Y=u\,(x-a)+v\,(y-b)$ $(sv-tu\neq 0)$ と表わせます. 隣の人の双曲線は $Y=1/X$ つまり $XY=1$ ですから, $(s\,(x-a)+t\,(y-b))(u\,(x-a)+v\,(y-b))=1$ と表わせます. 式を整理すると, $p\,(x-a)^2+q\,(x-a)(y-b)+r\,(y-b)^2=1$, ただし $p=su$, $q=sv+tu$, $r=tv$ です. このとき $q^2-4pr=(sv-tu)^2>0$ です. 方程式 $\boldsymbol{p\,(x-a)^2+q\,(x-a)(y-b)+r\,(y-b)^2=1}$ **(ただし $\boldsymbol{q^2-4pr>0}$)** が, **双曲線を表す方程式** です. 驚くべきことに, 楕円と双曲線は同じ形で条件 (q^2-4pr の正負) が異なるだけです.

2.5　放物線を表す方程式　最後に放物線ですが, 放物線は $y=x^2$ で表わされます. これまでと同じように, 隣の人の放物線 $Y=X^2$ をのぞき見すると, $X=s\,(x-a)+t\,(y-b)$, $Y=u\,(x-a)+v\,(y-b)$ $(sv-tu\neq 0)$ により, $u\,(x-a)+v\,(y-b)=(s\,(x-a)+t\,(y-b))^2$ と表わせます. 展開して整理して, $p\,(x-a)^2+q\,(x-a)(y-b)+r\,(y-b)^2-u\,(x-a)-v\,(y-b)=0$ $(p=s^2,\,q=2st,\,r=t^2)$ と表わせます. 前半は楕円や双曲線と同じ形ですが, $q^2-4pr=0$ です. 後半に 1 次の項がありますが, 楕円や双曲線ではこのような項はありませんでした. **放物線を表す方程式** としていろいろな形にできますが, $\boldsymbol{u\,(x-a)+v\,(y-b)=(s\,(x-a)+t\,(y-b))^2}$ とか, $\boldsymbol{p\,x^2+q\,xy+r\,y^2+u\,x+v\,y+w=0\ (q^2-4pr=0)}$ が適当でしょう.

§3　図形と有理点

座標平面上で, 直線, 円, 楕円, 双曲線, 放物線を表す方程式を与えました. ある方程式で与えられた図形に対して, 有理点 (x,y) (x, y は有理数) でその方程式を満たすものを, **その図形の上にある有理点** (あるいは単に, **その図形の有理点**) といいます. そもそも座標平面には, たくさんの有理点があります. 偏り無く, 隙間無く埋め尽くされているようにみえます. どんなに小さい部分にも, たくさんの有理点がびっしり詰まっています. ですから, 座標平面に適当に図形を描けば, その図形の上にはたくさんの有理点がのっているのではないでしょうか. 目の細かい方眼紙を用意していただいています. 方眼紙の目 (ここでは, 縦横の線の交わりを目と呼ぶことにします. 縦横の線で囲まれた四角い部分ではありません) を有理点に見立てて, 定規で直線を, コンパスで円を描いて, 方眼紙の目 (だいぶ荒いですが, 有理点) をたくさん通るように, 或いは全く通らないようにできますか? 普通, グラフを描くときは, グラフの通りそうな方眼紙の目の部分に点を描いてそれらを滑らかに結んでいることでしょう. もし, 有理点を全く通らない図形があったなら, それをどの様にして描けばいいのでしょうか.

3.1　直線と有理点　数学的には点も直線も曲線も大きさのない図形です. 鉛筆などで描いた線はある程度の大きさをもつので, 方眼紙の目の間隔が線の幅より小さくなると, 目を避けて線を描くことはできません. 数学的には線や曲線に大きさがないからと言っても, 有理点はびっしりと隙間が見えないぐらい並んでいます. 有理点と別の有理点の間に, 無数に多くに有理点があります. 有理点を避けて線や曲線を描くことができるのでしょうか.

> **定理**　直線 $p\,x+q\,y=r$ の上の有理点の個数は, 0 個か, 1 個か, 無数に多くのいずれかである.
> 係数の比 $p:q:r$ が有理数の比ならば無数に多くの有理点があり, 比 $p:q:r$ に無理数が現れれば
> 有理点の個数は多くて 1 個である.

直線の上に有理点がたくさん (無数に多く) あるかどうかは, その直線が有理数を係数とする方程式で表わされているかどうか, ということになります. 円, 楕円, 双曲線, 放物線に対しても, 係数に無理数が現れる場合は, ある種の数の関係でたまたま有理点をもつかどうかが問題となり, 係数に現れる無理数の特徴を調べることになります. この状況では, かなり難しい未解決問題に直面しますので, 今日はここには立ち入らないことにします. ここからは, 方程式の係数が有理数となるような円, 楕円, 双曲線, 放物線についてお話します.

3.2　放物線と有理点　放物線 $u\,(x-a)+v\,(y-b)=(s\,(x-a)+t\,(y-b))^2$ を展開し, x と y についてまとめると, $s^2\,(x-a)^2+2st\,(x-a)(y-b)+t^2\,(y-b)^2-u\,(x-a)-v\,(y-b)=0$ です. 係数が有理数になるとき, s^2, st, t^2 が有理数なので, 有理数 p, q, m で $s^2=m\,p^2$, $st=m\,p\,q$, $t^2=m\,q^2$ と表わせます. また u, v, a, b は有理数になります. 従って, この放物線は $u\,x+v\,y+w=m\,X^2$ $(X=p\,x+q\,y+r)$ で表わせます. X が有理数なら, $p\,x+q\,y=X-r$ も有理数で $u\,x+v\,y=m\,X^2-w$ も有理数です. これを連立方程式として x, y について解くとことで, 有理数の組 x, y が得られます. 放物線の上にいくらでも有理点を作ることができます.

3.3　円と有理点　次は, 円 $(x-a)^2+(y-b)^2=c$ です. 係数が有理数のものを考えていますので, 式を展開して整理して, a, b, c が有理数であることがわかります. (s,t) を円 $(x-a)^2+(y-b)^2=c$ の有理点とすると, $(s-a,t-b)$ で表される点は, 原点を中心とする円 $x^2+y^2=c$ の有理点です. 原点を中心とする円について調べれば十分です.

まずは単位円 $x^2+y^2=1$ からはじめましょう. 単位円は, x-軸, y-軸と $(\pm 1,0)$, $(0,\pm 1)$ で交わります. 単位円の有理点は他にも $(3/5,4/5)$, $(5/13,12/13)$ などがあります. どうやって見つけたのでしょうか. (s,t) $(\neq(1,0))$ を $x^2+y^2=1$ の有理点とします. (s,t) と $(1,0)$ を結ぶ直線 $t\,(x-1)-(s-1)\,y=0$ は有理点を 2 つもつので, その係数は有理数です. 有理点 (s,t) は有理数を係数とする直線と単位円とのです. ところで直線の方程式が有理数を係数にもつなら, 通分して分母を払うことで, 方程式の係数を整数にとれます. 直線 $m\,(x-1)+n\,y=0$ (m, n は

整数) と単位円 $x^2+y^2=1$ との交点を計算すれば, 単位円の上の有理点 $((m^2-n^2)/(m^2+n^2),\ 2mn/(m^2+n^2))$ が得られます. この技術は単純です. 有理点をひとつみつけたら, そこを通る直線を考え, 円との交点を調べるのです. 円でなくても, 直線との交点が基準とする有理点の他にもう 1 点ある場合に同じ技術が使えます.

定理　有理数係数の円, 楕円, 双曲線, 放物線が有理点をもつとき, 無数に多くの有理点をもつ.

この定理はかなり決定的な結果に見えます. あとは, 実際に一つでよいので有理点をみつけることです. 例えば, 円 $x^2+y^2=2$ では $(\pm1,\pm1)$, 円 $x^2+y^2=5$ では $(\pm1,\pm2)$, $(\pm2,\pm1)$, 円 $x^2+y^2=13$ では $(\pm2,\pm3)$, $(\pm3,\pm2)$ などなど. これらは, 適当に整数 x, y をとって x^2+y^2 を計算してまとめただけです. ところが不思議なことに x^2+y^2 の値に 3, 6, 7, 11, 12 などが現れないのです. x と y の範囲をいくら増やしても現れません. ということは, 円 $x^2+y^2=3$ や $x^2+y^2=6$, $x^2+y^2=7$ などは有理点をもたないのでしょうか?

3.4　楕円と有理点　楕円 $p\,(x-a)^2+q\,(x-a)(y-b)+r\,(y-b)^2=1$ $(q^2-4pr<0,\ p>0,\ r>0)$ を考えましょう. 係数が有理数になるのは p, q, r, a, b がすべて有理数のときです. 円のときと同様に, 楕円の中心が原点の場合を考えれば十分なので, 以下, $p\,x^2+q\,xy+r\,y^2=1$ $(q^2-4pr<0,\ p>0,\ r>0)$ について考えます . $p>0$ なので左辺を x について平方完成すると $p\,(x+(q/2p)\,y)^2-((q^2-4pr)/4p)\,y^2=1$ となります. ここで $q^2-4pr<0$, $p>0$ なので $-(q^2-4pr)/4p$ は正の有理数です. x と y がともに有理数であることと, $x+(q/2p)\,y$ と y がともに有理数であることは同じことなので, $p\,x^2+r\,y^2=1$ $(p>0,\ r>0)$ を考えれば十分です. 例えば $(p,r)=(1,2)$, $(1,3)$, $(2,3)$ の場合を考えてみましょう. 楕円 $x^2+2y^2=1$ や $x^2+3y^2=1$ には有理点 $(\pm1,0)$ があります. 円のところの定理から, $x^2+2y^2=1$ や $x^2+3y^2=1$ には無数に多くの有理点があります. 楕円 $2x^2+3y^2=1$ では, $\cdots$ (x,y) に適当に数を入れてみてもなかなかうまくいきません. 分母を通分して (x,y) として整数を考え $2x^2+3y^2$ の値が整数の二乗になっているのを探してみるのがいいかもしれません. x, y の範囲を ±100 まで, ±1000 までと拡げてみても, 有理点はみつかりません. この楕円に有理点はないのでしょうか.

3.5　双曲線と有理点　双曲線 $p\,(x-a)^2+q\,(x-a)(y-b)+r\,(y-b)^2=1$ $(q^2-4pr>0)$ についても, 式を展開して整理したときの係数がすべて有理数になるのは, p, q, r, a, b が有理数のときに限ります. 円や楕円のときと同様に, 双曲線の中心 (対称性の中心) が原点の場合を考えるので十分ですから, $p\,x^2+q\,xy+r\,y^2=1$ $(q^2-4pr>0)$ となります. $r=0$ のときは $x\,(p\,x+q\,y)=1$ ですから $p\,x+q\,y=1/x$. つまり $y=1/q(1/x-p\,x)$ となります. x を有理数とすれば, 自動的に y も有理数になり有理点がみつかります. あまりに単純です. $p=0$ の場合も同様ですから, 合わせて $pr\neq0$ の場合を考えましょう. $p\neq0$ なので $p\,x^2+q\,xy+r\,y^2=1$ の右辺を x について平方完成すると, $p\,(x-(q/2p)\,y)^2-((q^2-4pr)/4p)\,y^2=1$ となります. 双曲線として $p\,x^2-((q^2-4pr)/4p)\,y^2=1$ を考えれば十分です. 更に見やすい形にするために, 両辺 p で割って $1/p=n$, $(q^2-4pr)/4p^2=m$ とおくと, $x^2-m\,y^2=n$ となります. 双曲線にあるのは $m>0$ のときです. 幾つの例で有理点を調べてみましょう. 例えば $(m,n)=(1,1)$, $(2,1)$, $(2,-1)$, $(3,-1)$, $(3,2)$ としてみましょう. $x^2-y^2=1$ と $x^2-2y^2=1$ には有理点 $(\pm1,0)$ がありますから, 円のところの定理から, 無数に多くの有理点があります. 同様に $n=1$ のとき $x^2-m\,y^2=1$ は無数に多くの有理点をもちます. $x^2-2y^2=-1$ には有理点 $(1,1)$ がありますから, これも無数に多くの有理点をもちます. $x^2-3y^2=-1$ や $x^2-3y^2=2$ ではいかがでしょう. これらの双曲線の上に有理点はあるのでしょうか? ないのでしょうか?

更に不思議なことがあります. 無数に多くの有理点をもつ双曲線 $x^2-2y^2=1$ ですが, 実は無数に多くの格子点 (整数の座標をもつ点) を含むのです. 実際 $x^2-2y^2=1$ には $(1,0)$, $(3,2)$, $(17,12)$, $(99,70)$, $(577,408)$, $(3363,2378)$, $\cdots$ (x や y の符号を適当に変えたものも現れますが, 煩雑になるので符号は省きました) と, 格子点がたくさん見つかります. 円や楕円では, そもそもそれらはある程度の大きさの範囲に描かれるので, その範囲には有限個の格子点しかありませんから, このようかことは起こりません. とても不思議です.

定理　双曲線 $x^2-my^2=1$ (m は整数) は無数に多くの格子点を含む.

3.6　有理点が存在しないことの証明　円のところで述べた定理により, 円や楕円や双曲線では有理点が一つもないか, 無数に多くあるかのいずれかでした. たくさんあることを示すには, ともかく一つ有理点を見つければ十分でした. ひとつも無いことをどうやって証明すればいいのでしょうか. 有理数は無数にたくさんびっしり並んでいるので, 計算して有理点を探すにしても, 手当たり次第に適当に代入していくわけにはいきません. 何らかの規則に従って, 洩れのないように網羅的に調べていく必要があります.

楕円 $2x^2+3y^2=1$ の有理点をみつけるために, 分母を払って, 整数 x, y に対して $2x^2+3y^2$ が整数の二乗になるものを探しました. 2 つの有理数 x, y において, これらの分母の最小公倍数で通分して, $x=X/Z$, $y=Y/Z$ (X, Y, Z は整数) と表せます. $2x^2+3y^2=1$ にこれを代入して通分すると, $2X^2+3Y^2=Z^2$ となります. ここで X, Y に適当な範囲の整数を代入し, $2X^2+3Y^2$ が整数の二乗 (Z^2) になっているかどうかを調べたのでした. 整数の組 X, Y, Z が 1 以外の公約数 d を持てば, X/d, Y/d, Z/d も $x=(X/d)/(Z/d)$, $y=(Y/d)/(Z/d)$, $2(X/d)^2+3(Y/d)^2=(Z/d)^2$ をみたします. こうして, 整数の組 X, Y, Z は 1 以外の公約数をもたないようにできます. さて, $2X^2+3Y^2=Z^2$ は整数の方程式なので, 両辺を 3 で割ったあまりは等しい. $3Y^2$ は 3 の倍数なので, $2X^2$ と Z^2 を 3 で割ったあまりは等しい. 整数を 3 で割った余りは 0 (割り切れる), 1, 2 で, 整数の二乗を 3 で割ったあまりは, 0, 1 である. $2X^2$ を 3 で割ったあまりは 0 か 2 で, Z^2 を 3 で割った余りは 0 か 1 なので, $2X^2$ と Z^2 のそれぞれを 3 で割った余りが等しくなるのは, X も Z も 3 の倍数となるときに限る. このとき X^2, Z^2 は 9 の倍数です. $2X^2+3Y^2=Z^2$ より, Y もまた, 3 の倍数です. X, Y, Z が全て 3 の倍数となり, 1 以外の

公約数をもたないとしたことに反します. 有理数 x, y で $2x^2+3y^2=1$ をみたすものが存在するとの仮定が成り立たないことを意味します. 楕円 $2x^2+3y^2=1$ は有理点をもたないことが示されました.

この議論はとても有効です. 円 $x^2+y^2=3$, $x^2+y^2=6$, $x^2+y^2=7$ など, 楕円 $2x^2+5y^2=1$, $3x^2+7y^2=1$ など, 双曲線 $x^2-3y^2=-1$, $x^2-3y^2=2$ など, すべて同じようにして有理点をもたないことを証明できます. この議論のキーポイントは, 有理数の問題を整数の問題にしたことです. 円を含む楕円 $px^2+ry^2=1$ では $pX^2+rY^2=Z^2$ で. 双曲線 $x^2-my^2=n$ では $X^2-mY^2=nZ^2$ となります. 少し曖昧にしていましたが, 係数の p, r, m, n は有理数でした. 正しく整数の問題にするには, p, r, m, n についても通分して分母を払う必要があります. 楕円の場合は $\bigcirc X^2+\bigcirc Y^2=\bigcirc Z^2$, 双曲線では $\bigcirc X^2-\bigcirc Y^2=\bigcirc Z^2$ (それぞれ $\bigcirc$ には適当な整数が入る) となります. X, Y, Z の立場は異なりますが, 3 つの平方数の関係を表す同じ形の方程式であることに気づきます. 円, 楕円, 双曲線のそれぞれについて, その曲線上の有理点を調べる問題は, 整数 p, q, r に対して $pX^2+qY^2+rZ^2=0$ をみたす整数の組 (X,Y,Z) を調べる問題を少しずつ視点を変えてながめていたものなのです. 放物線をこの枠組みに入れるには, 少しややこしい式変形が必要です. 放物線が無数に多くの有理点ををもつことが有理点は既にすべてわかっていますから, 有理点を知るためにこの枠組みに組み込む必要はありません.

3.7　平方剰余　　円 $x^2+y^2=7$ は有理点をもちません. 上の, 楕円 $2x^2+3y^2=1$ が有理点をもたないことの証明をまねてみます. もし有理点をもっていたなら, $x=X/Z$, yY/Z (X, Y, Z は 1 以外に公約数をもたない整数) とおくと, $X^2+Y^2=7Z^2$ です. 右辺は 7 で割り切れるので, X^2+Y^2 は 7 で割り切れます. 従って, X^2 を 7 で割った余りと, Y^2 を 7 で割った余りの和は 7 で割り切れます. 少し見方を変えます. Y^2 を移項して $X^2=-Y^2+7Z^2$ とし, 7 で割った余りを考えます. X^2 を 7 で割った余りは, $-Y^2$ を 7 で割った余りに等しい. Y が 7 で割り切れるなら X も 7 で割り切れ, 結局 Z も 7 で割り切れてしまうので, Y は 7 で割り切れません.

Fermat の小定理　p を素数, a を p で割り切れない整数とする. a^{p-1} を p で割った余りは 1 に等しい

Fermat の小定理により, Y^6 を 7 で割った余りは 1 になります. $X^2=-Y^2+7Z^2$ の両辺を $(Y^5)^2$ 倍して, 7 で割った余りを考えます. 左辺は $X^2\times(Y^5)^2=(XY^5)^2$ なので, 整数の平方数を 7 で割った余りです. 右辺は (7 の倍数の $7Z^2(Y^5)^2$ は除いておいて) $-Y^2\times(Y^5)^2=-(Y^6)^2$ なので 7 で割った余りは -1 です (特に断り無く余りという用語を使うときは 6 と言うべきかもしれません). ここまで突き詰めていくと, 円 $x^2+y^2=7$ が有理点をもつかどうかは, ある整数の平方数を 7 で割った余りとして -1 が現れるかどうか, と言い換えることができます. これはもう, とんでもないことです. 無数に候補のある有理点の話が, 7 で割った余りの世界の話, たった 7 つの数の話になったのです. 0, 1, 2, 3, 4, 5, 6 を二乗して 7 で割った余りをとると, それぞれ 0, 1, 4, 2, 2, 4, 1 となり 6 (-1) は出てきません. 従って $x^2+y^2=7$ は有理点をもちません.

ある素数 p と, p で割り切れない整数 a について, a を p で割ったあまりがある整数の平方数を p で割った余りに等しいとき, a を法 p に関する **平方剰余** といいます. 平方剰余でないとき **平方非剰余** といいます. a が法 p に関する平方剰余のとき $(\frac{a}{p})=+1$, 平方非剰余のとき $(\frac{a}{p})=-1$ という記号を用意すると, 先ほどの -1 と 7 の関係は $(\frac{-1}{7})=-1$ で表せます. この記号を **平方剰余記号** といいます.

定理　p を 2 でない素数, a, b を p で割り切れない整数とする. このとき, 次が成り立つ.

$$(\tfrac{ab}{p})=(\tfrac{a}{p})(\tfrac{b}{p})$$

$$(\tfrac{-1}{p})=(-1)^{(p-1)/2}\quad (p\text{ が }4\text{ で割った余りが }1\text{ のとき }+1,\text{ 余りが }3\text{ のとき }-1)$$

更に p と異なる 2 でない素数 q について,

$$(\tfrac{p}{q})(\tfrac{q}{p})=(-1)^{(p-1)(q-1)/4}\quad (p\text{ も }q\text{ も }4\text{ で割った余りが }3\text{ のとき }-1\text{ でそれ以外では }+1)$$

かなり難しくなってきました. この定理から, 円について次のことがわかります. 5, 13, 17 など 4 で割った余りが 1 の素数 p について円 $x^2+y^2=p$ は無数に多くの有理点をもちます. 3, 7, 11 など 4 で割った余りが 3 の素数 p について円 $x^2+y^2=p$ は有理点をひとつももちません. 一般に $pX^2+qY^2+rZ^2=0$ をみたす整数の組があるかどうか, 平方剰余記号で表すことができます. 詳しくは書きません. 皆さんで考えてみてください.

§4　最後に

唐突に図形と有理数の関係という言葉から始まりましたが, そもそものきっかけは, 目の細かい方眼紙に何となく線を引いてみると, いつでも方眼紙の線の交差しているところを通っているように見えることでした. 交差点を通過しないように注意深く線を引いて, 次に円, 楕円, 双曲線, 放物線 ... 方眼紙に図形を描きながら, 感じたことを数学的にとらえようとして, 図形と有理数の漠然とした関係が見えてきて, 定式化のために図形の方程式を整備することから始めました. 図形を数学の枠組みでとらえたあとは, 数学技術の問題で, 余計なものをそぎ落とし本質をあらわにしていく作業です. 最後はとても単純な一つの方程式に帰着し, 問題を解決し, 次への発展を目指す. 今日の話しでは駆け足になりましたが, 何だか不思議だなぁ, 何だか面白いなぁ, と感じたところから始まるある種の研究手法の一端を紹介しました.

『 題材はふとした出会い, 心の動きを動機として, 「研究」してみませんか ？ 』