強者の戦略

それでは，前回の解答です．

第1問（Ⅲ C）

x 座標と y 座標がともに有理数である点を有理点という．

曲線 $y^2=x^3-x$ 上の有理点は

$(0,\ 0),\ (1,\ 0),\ (-1,\ 0)$

のみであることを示せ．

出題するときに載せていた誘導に沿って証明していきましょう．

(証明)

有理数 $a=\dfrac{m}{n}$ (既約分数) に対して，a の高さ $H(a)$ を $H(a)=\max(|m|,\ |n|)$ と定める．曲線 $y^2=x^3-x$ 上に上記以外の有理点が存在すると仮定し (そのような有理点は $y\neq 0$ を満たすことに注意)，x 座標の高さが最小となる $(x_0,\ y_0)$ をとり，これよりも x 座標の高さがさらに小さい有理点が作れることを示し矛盾を導く．証明は以下のステップで行う．

(a)　$(x,\ y)$ が曲線 $y^2=x^3-x$ 上の $(0,\ 0)$ 以外の有理点であるとき，$\left(-\dfrac{1}{x},\ \dfrac{y}{x^2}\right)$ も曲線上にある有理点になるので，これから $x_0>1$ としてよいことを示す．

(b)　$x_0>1$ として，$x_0=\dfrac{m}{n},\ m>n>0$ と既約分数表示すると，m と n の一方は偶数，一方は奇数となることを示す．

(c)　$y_0^{\,2}=x_0^{\,3}-x_0=x_0(x_0+1)(x_0-1)$ となるが，x_0，x_0+1，x_0-1 のそれぞれが有理数の平方となることを示す．

(d)　前回の問題で定義した合成写像 $h\circ g : B\to D$ は全射なので

$h\circ g(x_1,\ y_1)=(x_0,\ y_0)$

となる有理点 $(x_1,\ y_1)$ が存在する．この x_1 が

$H(x_1)<H(x_0)$

を満たすことを示す．

(a) について

$(x,\ y)$ が曲線 $y^2=x^3-x$ 上の $(0,\ 0)$ 以外の有理点であるとき，$\left(-\dfrac{1}{x},\ \dfrac{y}{x^2}\right)$ は有理点であり，これを $(X,\ Y)$ とおくと

$$X^3-X=\left(-\frac{1}{x}\right)^3-\left(-\frac{1}{x}\right)=\frac{x^3-x}{x^4}=\frac{y^2}{x^4}=Y^2$$

なので，$(X,\ Y)$ も曲線 $y^2=x^3-x$ 上の有理点である．

$$H(x)=H\left(-\frac{1}{x}\right)$$

が成り立つので，必要ならば x_0 を $-\dfrac{1}{x_0}$ と取り替えて，$x_0>0$ としてよい．すると

$$y_0^{\,2}=x_0(x_0+1)(x_0-1)>0$$

なので $x_0>1$ としてよい．

(b) について

$x_0>1$ として，$x_0=\dfrac{m}{n},\ m>n>0$ と既約分数表示する．m，n がどちらも奇数として矛盾を導く．

$$x_0'=\frac{x_0+1}{x_0-1}=\frac{(m+n)/2}{(m-n)/2}$$

として，点 $\left(x_0',\ \dfrac{2y_0}{(x_0-1)^2}\right)$ を考えると

$$\begin{aligned}(x_0')^3-x_0' &= \frac{(x_0+1)^3}{(x_0-1)^3}-\frac{x_0+1}{x_0-1}\\ &= \frac{(x_0+1)\left((x_0+1)^2-(x_0-1)^2\right)}{(x_0-1)^3}\\ &= \frac{4x_0(x_0+1)(x_0-1)}{(x_0-1)^4}\\ &= \left(\frac{2y_0}{(x_0-1)^2}\right)^2\end{aligned}$$

なので，点 $\left(x_0',\ \dfrac{2y_0}{(x_0-1)^2}\right)$ も曲線 $y^2=x^3-x$ 上の有理点である．ところが

強者の戦略

$$H(x_0')\leqq \max\left(\frac{m+n}{2},\frac{m-n}{2}\right)$$
$$<\max(m,n)$$
$$=H(x_0)$$

であるので，これではx_0の高さの最小性に反する．よって，m，nがともに奇数になることはなく，さらにm，nは互いに素なのでともに偶数であることもない．従って，m，nのうち一方は偶数，もう一方は奇数である．

(c) について

$$y_0{}^2=x_0(x_0+1)(x_0-1)=\frac{m(m+n)(m-n)}{n^3}$$

となる．まず，m，n，$m+n$，$m-n$がどの2つも互いに素であることを示す．m，nが互いに素であることから，互いに素でない可能性があるのは$m+n$と$m-n$の組だけであるが，これらの公約数をdとすると，dは$(m+n)+(m-n)=2m$と$(m+n)-(m-n)=2n$をどちらも割り切り，mとnが互いに素であることから，$d=1$または2となる．さらに，(2)で示したようにm，nの偶奇は異なるので$d=2$とはなりえず，$d=1$，すなわち$m+n$と$m-n$も互いに素である．

すると，$\dfrac{m(m+n)(m-n)}{n^3}$は既約分数で有理数の平方であることからm，n，$m+n$，$m-n$はいずれも平方数になり

$$x_0=\frac{m}{n},\ x_0+1=\frac{m+n}{n},\ x_0-1=\frac{m-n}{n}$$

はそれぞれが有理数の平方である．

(d) について

(前々回に出題した問題を用いるので，右側にもう一度載せておきます．)

問（Ⅲ C）

$\mathbb{Q}$を有理数全体の集合とし，集合A，B，C，Dを次のように定める．

$A=\{(s,\ t,\ u)\,|\,s,\ t,\ u\in\mathbb{Q},\ s^2+1=t^2=u^2-1\}$

$B=\{(x,\ y)\,|\,x,\ y\in\mathbb{Q},$
$y^2=x(x+1)(x-1),\ y\neq 0\}$

$C=\{(x,\ y)\,|\,x,\ y\in\mathbb{Q},\ y^2=x(x+1)(x-1)\}$

$D=\{(x,\ y)\,|\,x,\ y\in\mathbb{Q},\ y^2=x(x+1)(x-1)$
かつx，$x+1$，$x-1$はどれも$\mathbb{Q}$の平方元$\}$

また，写像$f:A\to B$，$g:B\to A$，$h:A\to C$を次のように定める．

$f(s,\ t,\ u)$
$=(s^2+1+st+tu+us,\ (s+t)(t+u)(u+s))$

$$g(x,\ y)=\left(\frac{x^2-2x-1}{2y},\ \frac{x^2+1}{2y},\ \frac{x^2+2x-1}{2y}\right)$$

$h(s,\ t,\ u)=(s^2+1,\ stu)$

このとき，以下の設問に答えよ．

(1) (2)　略

(3)　合成写像$h\circ g:B\to C$の像はDに一致することを示せ．

(c) から$(x_0,\ y_0)$は上記の問題の集合Dの元である．すると (3) より$(x_1,\ y_1)\in B$で

$h\circ g(x_1,\ y_1)=(x_0,\ y_0)$

となるものが存在する．写像g，hの定義より

$$x_0=\left(\frac{x_1{}^2-2x_1-1}{2y_1}\right)^2+1=\frac{(x_1{}^2+1)^2}{4x_1(x_1+1)(x_1-1)}$$

であり，$x_1=\dfrac{r}{s}$と既約分数で表すと

$$x_0=\frac{(r^2+s^2)^2}{4rs(r^2-s^2)}$$

となる．

このとき，x_0の分母と分子の最大公約数は4以下であることをまず示す．r^2+s^2とr^2-s^2の公約数をdとすると，dは$2r^2$，$2s^2$をともに割り切り，r^2とs^2は互いに素であることから，$d=1$または2である．

よって，分母と分子の最大公約数は 2 のベキ乗になる．r^2+s^2 が偶数になるとき，r，s はともに奇数なので r^2，s^2 を 4 で割った余りはともに 1 で r^2+s^2 を 4 で割った余りは 2 となり，$(r^2+s^2)^2$ は 8 では割り切れない．よって，x_0 の分母と分子の最大公約数は 4 以下である．

これから

$$\begin{aligned} H(x_0) &\geqq \frac{1}{4}(r^2+s^2)^2 \\ &\geqq \frac{1}{4}\Big(\max(|r|,|s|)\Big)^4 \\ &> \max(|r|,|s|) \\ &= H(x_1) \end{aligned}$$

となるが，これは $H(x_0)$ の最小性に反する (最後の不等式は $x_1 \neq 0, \pm 1$ より，$H(x_1) \geqq 2$ であることによる).

以上より，有理点 $(x_0,\ y_0)$ は存在せず題意が示せた．

□

(コメント)

今回は，見た目はシンプル，証明はハードな問題に挑戦してもらいました．誘導に乗れたでしょうか？

証明に用いる手法は前々回に練習してもらった

“無限降下法”

です．自然数であれば，大小で順序が入りますのですぐに降下法に持ち込めるのですが，今回は相手が有理数ですので高さ $H(a)$ を準備して，これに降下法を使いました．$(x_0,\ y_0)$ を x 座標の高さが最小になるような有理点として，前回に準備した写像から $(x_1,\ y_1)$ という x 座標の高さがもっと小さい有理点が存在することを示します．以下証明の各ステップごとの補足です．

(a)　高さ関数の性質として

$$H(x)=H\Big(-\frac{1}{x}\Big)$$

が成り立つことから，$x_0>0$　で考えてよいことが分かります．すると，$y_0^{\,2}>0$ より $x_0>1$ となります．

(b)　x_0 を既約分数表示したとき，分母・分子がともに奇数として矛盾を導きます．x_0' を与えられたようにとると，分母・分子がともに奇数であれば高さが x_0 より小さくなってしまうことが言えます．ここにも降下法を使っています．

$$\begin{aligned} H(x_0') &\leqq \max\Big(\frac{m+n}{2},\frac{m-n}{2}\Big) \\ &< \max(m,n) \\ &= H(x_0) \end{aligned}$$

の最初の不等号は $\dfrac{m+n}{2}$，$\dfrac{m-n}{2}$ が互いに素なとき等号が成立し，2 番目の不等号は $m \neq n$ なので等号になることはありません．

(c)　(b) で m，n の偶奇が異なることが言えているので，$m+n$，$m-n$ が互いに素になり，これから x_0，x_0-1，x_0+1 がどれも有理数の平方になることに示せます．これによって，$(x_0,\ y_0)$ が前回の問題の集合 D に属することが分かります．

(d)　前回の問題で，D への全射が作れていましたので，これを使って，$(x_0,\ y_0)$ から有理点 $(x_1,\ y_1)$ がとれます．$(x_1,\ y_1)$ を具体的に書くのは大変ですが，存在は保証されるので，あとは x_0 と x_1 の関係式から

$$H(x_1)<H(x_0)$$

を示せば OK です．

前回の解説時にも書きましたが

$$y^2=(x-a)(x-b)(x-c)$$

$(a,\ b,\ c$ は相異なる $\mathbb{Q}$ の元)

という関数のグラフを $\mathbb{Q}$ 上の楕円曲線といいます．楕円曲線上の有理点は古くから数論の研究対象として深く研究されてきました．というのは，これらの有理点には“和”が定義でき，有理点と有理点を“足す”ことで，別の有理点を作れたりするのです（数学的には群の構造が入ると言います）．証明中に出

強者の戦略

てきた $\left(-\frac{1}{x},\ \frac{y}{x^2}\right)$ や $\left(x_0',\ \frac{2y_0}{(x_0-1)^2}\right)$ は突然出てきてびっくりしたかもしれませんが，実はこの“和”を計算することで求まるものです．

最後に，「有理点が求まったら何が面白いの？」「だから何やねん？」と思っている人へ，この定理から直ちに得られる有名な結果をお見せします．

> 系 (フェルマーの最終定理の $n=4$ の場合)
> 自然数 x，y，z で
> $x^4+y^4=z^4$ …… (*)
> を満たすものは存在しない．

（証明）

背理法で示す．自然数 x，y，z で (*) を満たすものが存在すると仮定する．すると

$$\begin{aligned} x^4+y^4=z^4 &\iff x^4=z^4-y^4 \\ &\iff \frac{x^4z^2}{y^6}=\frac{z^6}{y^6}-\frac{z^2}{y^2} \\ &\iff \left(\frac{x^2z}{y^3}\right)^2=\left(\frac{z^2}{y^2}\right)^3-\frac{z^2}{y^2} \end{aligned}$$

となり，これでは曲線 $y^2=x^3-x$ 上に $y\neq 0$ となる有理点が存在することになり，上で示した定理に反する．

□

フェルマーの最終定理とは

> n を 3 以上の自然数とするとき，自然数 x，y，z で
> $x^n+y^n=z^n$
> を満たすものは存在しない．

というもので，$n=3$，4，5 の場合などは証明が知られていましたが，一般の n の場合は長い間未解決で，1995 年に A.Wiles によってようやく証明されました．今回示した定理は，この定理の $n=4$ の場合を含んでいます．楕円曲線からフェルマーの最終定理が出てくるのは興味深いですね．

実は，フェルマーの最終定理を Wiles が証明した方法も楕円曲線を用いるものでした．$a^n+b^n=c^n$ を満たす自然数 a，b，c があったと仮定して

$y^2=x(x-a^n)(x+b^n)$

という楕円曲線を考えます (フライ曲線と呼ばれています)．この曲線が，楕円曲線が必ず持たなくてはならない“モジュラー”という性質を持ち得ないということを示すことで最終定理は証明されます．現代数学の道具を駆使して 100 頁以上の大論文ですので，読むのは大変ですが，興味のある人は大学に入ってから（もっと早い人は高校生のうちに？）勉強してみてください．

なお，今回の証明は

加藤和也・黒川信重・斉藤毅　著

『数論 1　Fermat の夢』(岩波書店)

にあるものに，細部の説明を書き加えたものです．この本には ζ や代数的整数論といった，整数論の基本テーマが分かりやすく書かれていますので，興味のある人は手に取ってみてください (大学生になってからで構いません)．

それでは今回はここまでにしたいと思います．次回をお楽しみに．

（数学科　川﨑）