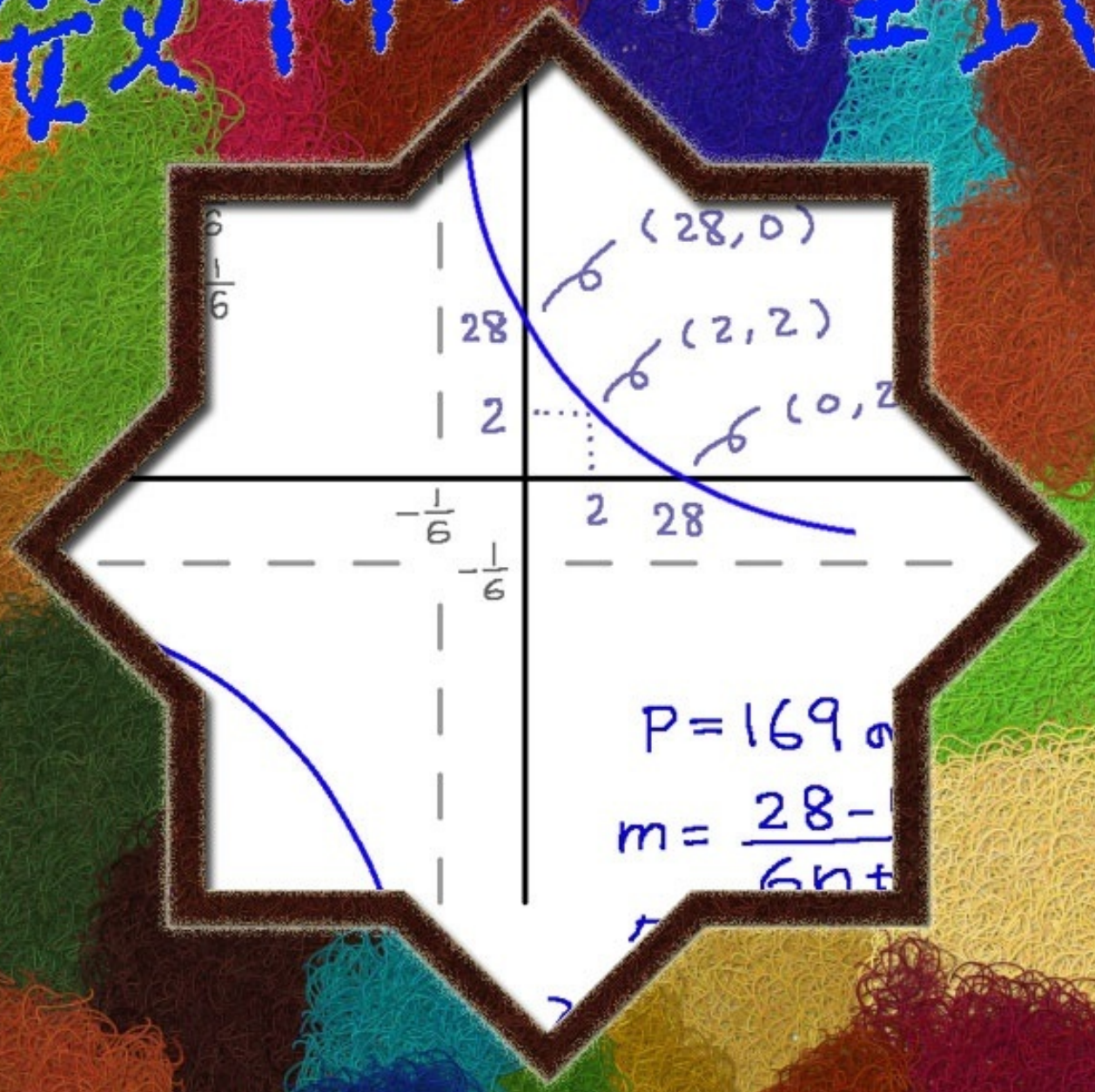
茜町春彦

エッセイ（数学）

素数判定方程式



エッセイ（数学）

『素数判定方程式』

著者：茜町春彦

概要：
素数を判定するための方程式（ディオファントス方程式）を紹介します．
つづいて、その導き方と使い方を説明します．ただし、２と３が素数かどうかをこの方程式では判定できませんが、これらを今さら判定しても意味は無いので、２と３は例外とします．また証明は行なっておりません．ご了承ください．

読者対象：
整数論やＲＳＡ暗号に興味のある方．

目次：

素数判定方程式、Ｐ＝３６ｍｎ＋６ｍ＋６ｎ＋１の概略

素数判定方程式を示して、概略を説明します．
（導き方と使い方は後述します．また素数２と素数３は除外します）

Ｐ＝３６ｍｎ＋６ｍ＋６ｎ＋１

Ｐには、素数かどうかを判定したい数を代入します．
ｍとｎは、変数です．

この素数判定方程式に、或る数Ｐを与えて、ｍとｎの整数解を求めます．その結果により、Ｐが素数かどうかを判定します．

判定基準は、ｍとｎの整数解が共に０以外であれば、Ｐは合成数と判定します．
なぜなら、
Ｐ＝３６ｍｎ＋６ｍ＋６ｎ＋１＝（６ｍ＋１）×（６ｎ＋１）
となり、Ｐが素因数分解できるからです．

ｍとｎの整数解が共に０になるのは、Ｐ＝１の場合だけです．
なぜなら、
Ｐ＝３６×０×０＋６×０＋６×０＋１＝１
となるからです．

上記以外の場合、つまり、ｍとｎの片方だけが０となる整数解しかない場合、Ｐは素数と判定します．
Ｐ＝（３６ｍ×０）＋６ｍ＋（６×０）＋１＝６ｍ＋１
または
Ｐ＝（３６×０×ｎ）＋（６×０）＋６ｎ＋１＝６ｎ＋１
となり、素因数分解ができないからです．

例として、９１が素数か合成数かを判定してみます．
素数判定方程式のＰに９１を代入します．

９１＝３６ｍｎ＋６ｍ＋６ｎ＋１

この式の整数解を求めると、（ｍ、ｎ）＝（１、２）があります．
整数解が共に０以外なので、Ｐは合成数であり、素因数分解ができます．

Ｐ＝（６ｍ＋１）×（６ｎ＋１）

９１＝（６×１＋１）×（６×２＋１）＝７×１３

となります.

素数判定方程式の導き方を説明します（その一）

すべての素数が ｜６Ｎ＋１｜ の形で表せることを示します.
（Ｎ＝０、±1、±2、±3、±4、・・・）
（記号｜　｜は絶対値を表します）

まず、整数を六つに分類します.
６で割ったときの余りに基づいて分類します.
つまり、６Ｎ、６Ｎ＋１、６Ｎ＋２、６Ｎ＋３、６Ｎ＋４、６Ｎ＋５の六つの分類です.

６Ｎ　　：　・・・、－１８、－１２、－６、０、　６、１２、１８、２４、・・・
６Ｎ＋１：　・・・、－１７、－１１、－５、１、　７、１３、１９、２５、・・・
６Ｎ＋２：　・・・、－１６、－１０、－４、２、　８、１４、２０、２６、・・・
６Ｎ＋３：　・・・、－１５、　－９、－３、３、　９、１５、２１、２７、・・・
６Ｎ＋４：　・・・、－１４、　－８、－２、４、１０、１６、２２、２８、・・・
６Ｎ＋５：　・・・、－１３、　－７、－１、５、１１、１７、２３、２９、・・・

ここで絶対値を取ってみると：
｜６Ｎ｜　　６の倍数　（素数ではない）
｜６Ｎ＋１｜　　素数または合成数
｜６Ｎ＋２｜＝｜２×（３Ｎ＋１）｜　　２の倍数　（素数ではない）
｜６Ｎ＋３｜＝｜３×（２Ｎ＋１）｜　　３の倍数　（素数ではない）
｜６Ｎ＋４｜＝｜２×（３Ｎ＋２）｜　　２の倍数　（素数ではない）
｜６Ｎ＋５｜　　素数または合成数
となります.

｜６Ｎ｜と｜６Ｎ＋２｜と｜６Ｎ＋３｜と｜６Ｎ＋４｜は、偶数または３の倍数となるので、素数ではありません.

従って素数は、｜６Ｎ＋１｜もしくは｜６Ｎ＋５｜の形となります.

｜６Ｎ＋１｜　・・・、｜－１７｜、｜－１１｜、｜－５｜、１、　７、１３、１９、２５、・・・

｜６Ｎ＋５｜　・・・、｜－２５｜、｜－１９｜、｜－１３｜、　｜－７｜、｜－１｜、５、１１、１７、・・・

｜６Ｎ＋１｜と｜６Ｎ＋５｜の内容は全く同じであることから、どちらか一方を考察するだけで素数の判定ができます．このエッセイに於いては、｜６Ｎ＋１｜を使って考察を行なうことにします．

また絶対値をつけたままで考察を続けても構わないのですが、計算式の取り扱いをさらに単純化するために、｜６Ｎ＋１｜から絶対値の記号を外して考察をすることにします．そのかわり、負号は無視することにします．例えば、「－５」は「５」と見なし、「－１１」は「１１」と見なし、「－３５」は「３５」などと見なすと云うことです．

繰り返して言いますと、負号を無視すると全ての素数は、６Ｎ＋１の形に表せると云うことです．

Ｐ＝６Ｎ＋１、（Ｎ＝０、±1、±2、±3、±4、・・・）

・・・、－２９、－２３、－１７、－１１、－５、１、　７、１３、１９、２５、３１、３７、４３，４９、５５，６１、・・・

素数判定方程式を導き方を説明します（その二）

６Ｎ＋１ の形の整数同士の積も、６Ｎ＋１ の形で表せることを示します.

まず、ふたつの６Ｎ＋１ の形の整数を考えます.

Ｐ’＝６ｍ＋１
Ｐ’’＝６ｎ＋１
（ｍ、ｎ＝０、±１、±２、±３、±４、・・・）

そして、Ｐ’とＰ’’の積を考えます.
Ｐ’×Ｐ’’＝（６ｍ＋１）×（６ｎ＋１）＝３６ｍｎ＋６ｍ＋６ｎ＋１＝６×（６ｍｎ＋ｍ＋ｎ）＋１
となります.

ここで、（６ｍｎ＋ｍ＋ｎ）をＮと置きます.
すると、
Ｐ’×Ｐ’’＝６Ｎ＋１
となります.

つまり、６Ｎ＋１の形の整数同士の積もまた６Ｎ＋１の形になっている事が分かります.
Ｐ’×Ｐ’’＝６Ｎ＋１＝Ｐ＝３６ｍｎ＋６ｍ＋６ｎ＋１
と云うことです.

この右辺の二つの項を、素数判定方程式と呼ぶことにします.
Ｐ＝３６ｍｎ＋６ｍ＋６ｎ＋１
です.

素数判定方程式の使い方を説明します

素数判定方程式
Ｐ＝３６ｍｎ＋６ｍ＋６ｎ＋１
の使い方を説明します．

素数かどうかを判定したい数をＰとします．

まず、Ｐを６で割ったときの余りを求めます．

その結果、余りが１であればＰを素数判定方程式に代入して、ｍとｎの整数解を求めます．
余りが５であれば、Ｐに負号をつけたものを素数判定方程式に代入して、ｍとｎの整数解を求めます．

ｍとｎが共に０以外の整数解があればＰは合成数であり、なければ素数となります．
（ｍ、ｎ共に０になるのはＰ＝１のときだけです）

余りが０、２、３、４の場合、Ｐは偶数か３の倍数です．

使い方は以上ですが、もう少し補足してみます．

ｍ≠０かつｎ≠０となる整数解が見つかれば、Ｐは合成数と判定します．
Ｐ’＝６ｍ＋１
Ｐ’’＝６ｎ＋１
Ｐ＝Ｐ’×Ｐ’’＝（６ｍ＋１）×（６ｎ＋１）
となり、素因数分解ができるからです．

ｍ＝０かつｎ≠０しか整数解がない場合は、Ｐは素数と判定します．
Ｐ’＝６ｍ＋１＝６×０＋１＝１
Ｐ’’＝６ｎ＋１
Ｐ＝Ｐ’×Ｐ’’＝１×（６ｎ＋１）＝６ｎ＋１
となり、素因数分解ができないからです．

同様に、ｍ≠０かつｎ＝０しか整数解がない場合も、Ｐは素数と判定します．
Ｐ’＝６ｍ＋１
Ｐ’’＝６ｎ＋１＝６×０＋１＝１
Ｐ＝Ｐ’×Ｐ’’＝（６ｍ＋１）×１＝６ｍ＋１

となり、素因数分解ができないからです.

以上のように判定を行ないます.

計算例、Ｐ＝１６９の場合

素数判定方程式を使って、実際に計算をしてみます.

１６９が素数なのか合成数なのかの判定は、次のように行ないます.

１６９は６で割ると１余るので、６Ｎ＋１の形をしています.
そこで１６９を素数判定方程式のＰに代入しますと、
１６９＝３６ｍｎ＋６ｍ＋６ｎ＋１
となります.

この方程式のｍとｎの整数解を求めます.
ｍとｎに０以外の整数解があれば、Ｐは合成数であり、なければ素数となります.

この方程式を満たす整数解には、
（ｍ、ｎ）＝（２、２）
があります. 従って、１６９は合成数です.

Ｐ’＝６ｍ＋１＝６×２＋１＝１３
Ｐ’’＝６ｎ＋１＝６×２＋１＝１３

つまり、
Ｐ＝１６９＝Ｐ’×Ｐ’’＝１３×１３
と素因数分解できます.

図式解法：Ｐ＝１６９の場合

計算の代わりに図を使って判定する方法を紹介します.

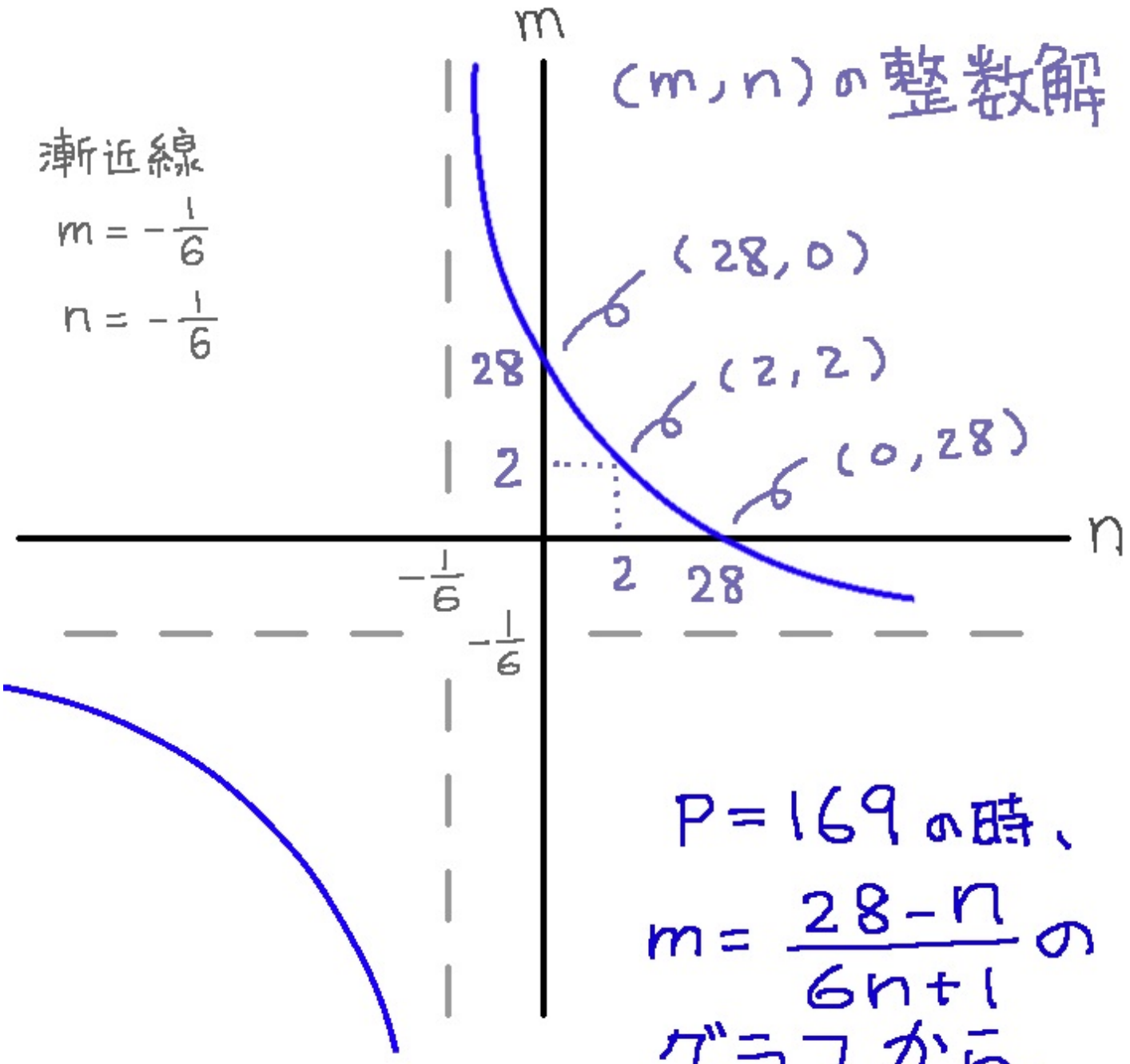
１６９＝３６ｍｎ＋６ｍ＋６ｎ＋１

この素数判定法定式を次のように変形します.

１６９－１＝３６ｍｎ＋６ｍ＋６ｎ
１６８＝３６ｍｎ＋６ｍ＋６ｎ
１６８÷６＝（３６ｍｎ＋６ｍ＋６ｎ）÷６
２８＝６ｍｎ＋ｍ＋ｎ
２８＝ｍ（６ｎ＋１）＋ｎ
２８－ｎ＝ｍ（６ｎ＋１）
（２８－ｎ）÷（６ｎ＋１）＝ｍ
ｍ＝（２８－ｎ）÷（６ｎ＋１）

縦軸をｍ、横軸をｎとして、上記の最後の式をグラフを書いて整数解を求めます.

グラフ：Ｐ＝１６９の場合



P=169の時、

$m=\frac{28-n}{6n+1}$ の

グラフから、

(m,n)=(2,2)を見つけます.

6m+1=13

6n+1=13 となりますので"

169=13×13 となります.

計算例、Ｐ＝９７の場合

９７が素数なのか合成数なのかの判定は、次のように行ないます.

９７は６で割ると１余るので、６Ｎ＋１の形をしています.

そこで９７を素数判定方程式のＰに代入しますと、
９７＝３６ｍｎ＋６ｍ＋６ｎ＋１
となります.

この方程式のｍとｎの整数解を求めます.
ｍとｎに０以外の整数解があれば、Ｐは合成数であり、なければ素数となります.

この方程式を満たす整数解は、
（ｍ、ｎ）＝（０、１６）もしくは（１６、０）
だけしかありません．従って、９７は素数です.

Ｐ’＝６ｍ＋１＝６×０＋１＝１
Ｐ’’＝６ｎ＋１＝６×１６＋１＝９７
つまり、
Ｐ＝９７＝Ｐ’×Ｐ’’＝１×９７
となり、素因数分解ができません.

図式解法：Ｐ＝９７の場合

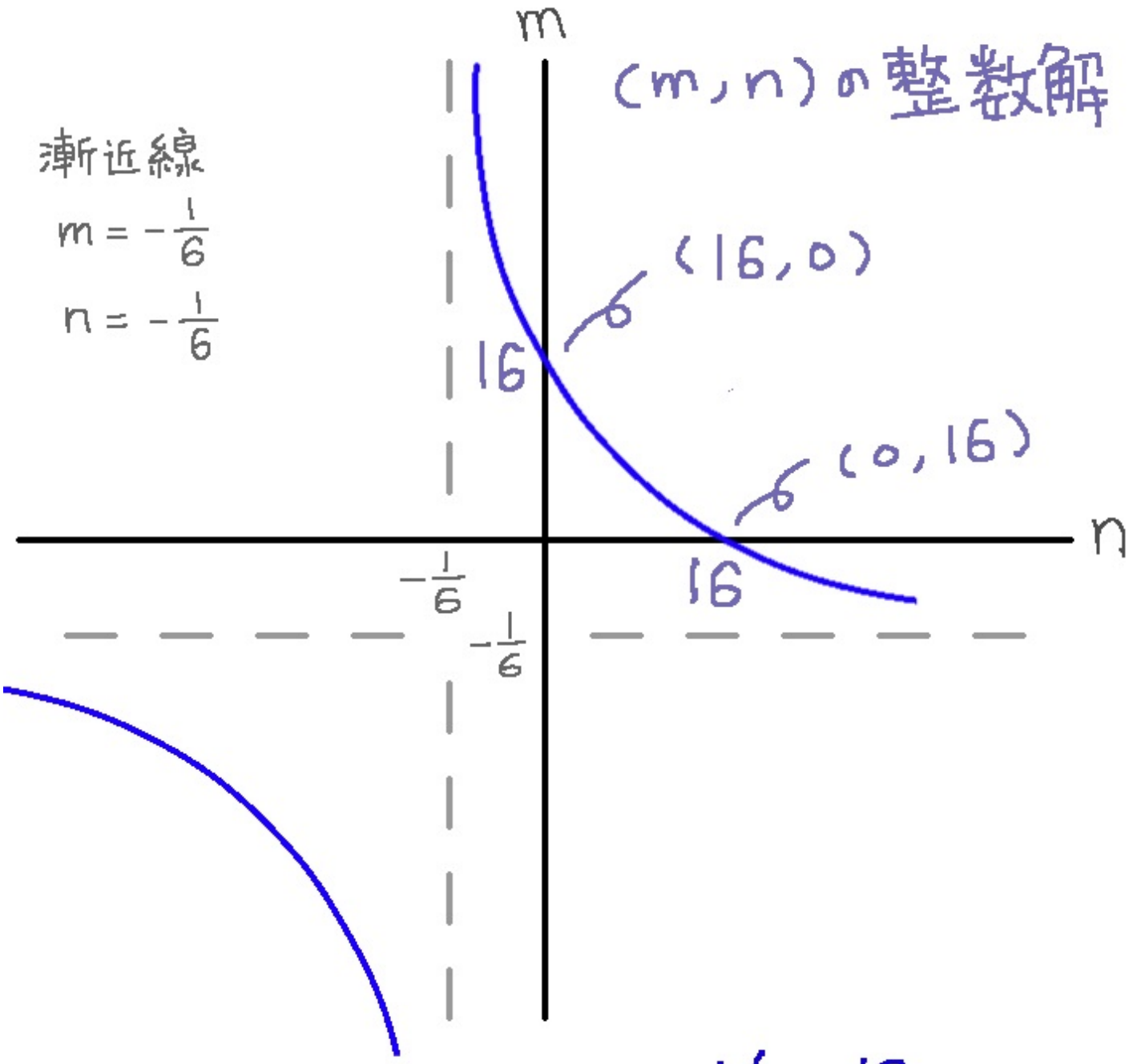
９７＝３６ｍｎ＋６ｍ＋６ｎ＋１

この素数判定法定式を次のように変形します.

９７－１＝３６ｍｎ＋６ｍ＋６ｎ
９６＝３６ｍｎ＋６ｍ＋６ｎ
９６÷６＝（３６ｍｎ＋６ｍ＋６ｎ）÷６
１６＝６ｍｎ＋ｍ＋ｎ
１６＝ｍ（６ｎ＋１）＋ｎ
１６－ｎ＝ｍ（６ｎ＋１）
（１６－ｎ）÷（６ｎ＋１）＝ｍ
ｍ＝（１６－ｎ）÷（６ｎ＋１）

縦軸をｍ、横軸をｎとして、上記の最後の式をグラフを書いて整数解を求めます.

グラフ：Ｐ＝９７の場合



P=97の時、$m=\frac{16-n}{6n+1}$ の整数解は (0,16) または (16,0) だけなので、97は素数です.

計算例、Ｐ＝１０１の場合

１０１が素数なのか合成数なのかの判定は、次のように行ないます.

１０１は６で割ると５余るので、６Ｎ＋１の形ではありませんが、６Ｎ＋５の形をしているので、負号をつけてー１０１として判定を行ないます.

ー１０１は６で割ると１余るので６Ｎ＋１の形になっています.
ー１０１＝６×（ー１７）＋１

そこで、ー１０１を素数判定方程式のＰに代入しますと、
ー１０１＝３６ｍｎ＋６ｍ＋６ｎ＋１
となります.

このｍとｎの整数解を求めます.
ｍとｎに０以外の整数解があれば、Ｐは合成数であり、なければ素数となります.

この方程式を満たす整数解は、
（ｍ、ｎ）＝（０、ー１７）もしくは（ー１７、０）
だけしかありません.
従って、ー１０１は素数です.（負号を無視して、１０１と心の中で解釈しておきます）

Ｐ’＝６ｍ＋１＝６×０＋１＝１
Ｐ’’＝６ｎ＋１＝６×（ー１７）＋１＝ー１０１
つまり、
Ｐ＝ー１０１＝Ｐ’×Ｐ’’＝１×（ー１０１）
となり、素因数分解できません.

図式解法：Ｐ＝１０１の場合

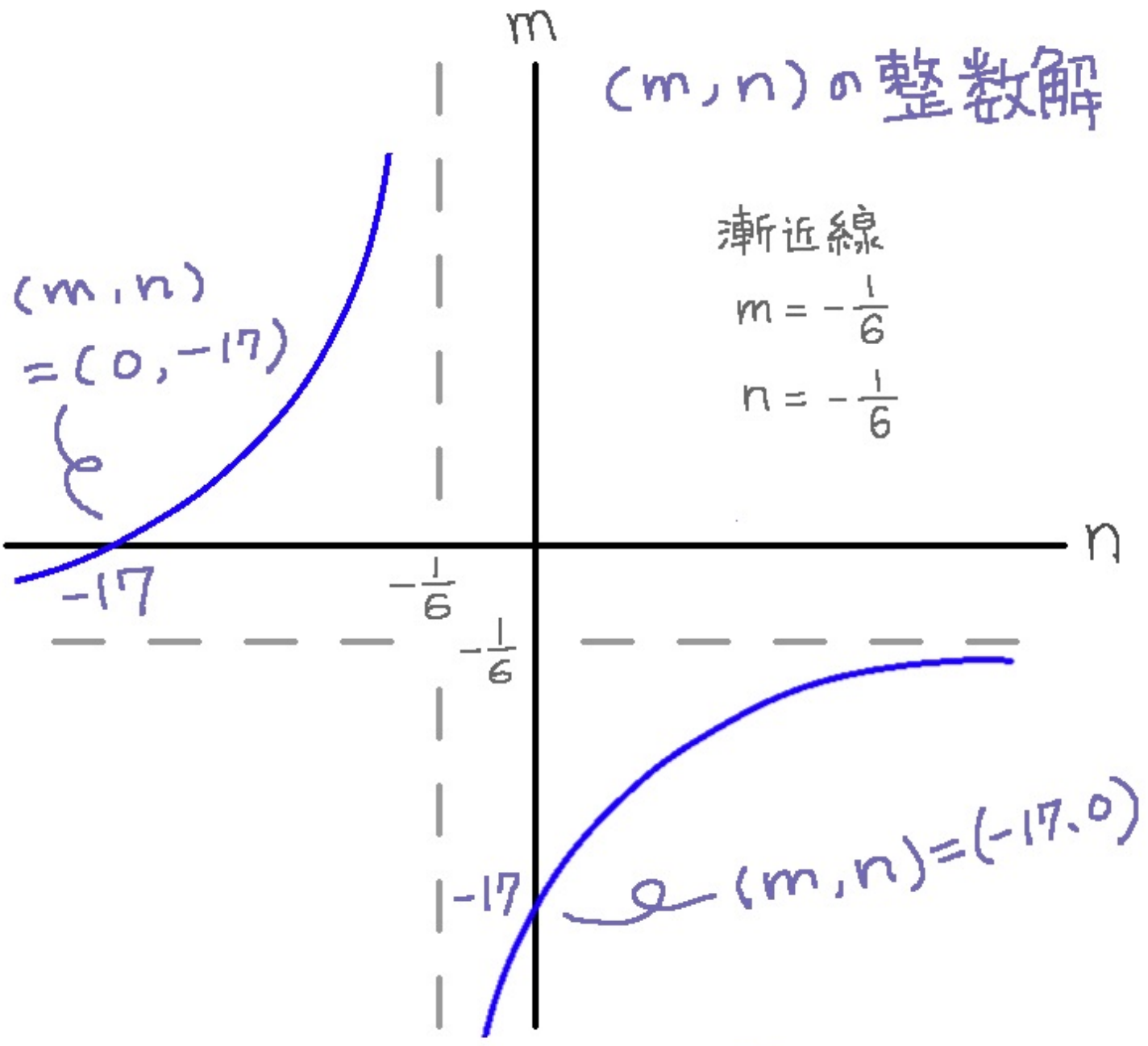
－１０１＝３６ｍｎ＋６ｍ＋６ｎ＋1

この素数判定法定式を次のように変形します.

－１０１－１＝３６ｍｎ＋６ｍ＋６ｎ
－１０２＝３６ｍｎ＋６ｍ＋６ｎ
－１０２÷６＝（３６ｍｎ＋６ｍ＋６ｎ）÷６
－１７＝６ｍｎ＋ｍ＋ｎ
－１７＝ｍ（６ｎ＋１）＋ｎ
－１７－ｎ＝ｍ（６ｎ＋１）
（－１７－ｎ）÷（６ｎ＋１）＝ｍ
ｍ＝（－１７－ｎ）÷（６ｎ＋１）

縦軸をｍ、横軸をｎとして、上記の最後の式をグラフを書いて整数解を求めます.

グラフ：Ｐ＝１０１の場合



$P=101$の時、$m=\frac{-17-n}{6n+1}$の整数解は$(0,-17)$または$(-17,0)$だけなので、101は素数です。

計算例、Ｐ＝１８７の場合

１８７が素数なのか合成数なのかの判定は、次のように行ないます.

１８７は６で割ると１余るので、６Ｎ＋１の形をしています.
そこで１８７を素数判定方程式のＰに代入しますと、
１８７＝３６ｍｎ＋６ｍ＋６ｎ＋１
となります.

この方程式のｍとｎの整数解を求めます.
ｍとｎに０以外の整数解があれば、Ｐは合成数であり、なければ素数となります.

この方程式を満たす整数解には、
（ｍ、ｎ）＝（－２、－３）
があります. 従って、１８７は合成数です.

Ｐ’＝６ｍ＋１＝６×（－２）＋１＝－１１
Ｐ’’＝６ｎ＋１＝６×（－３）＋１＝－１７
つまり、
Ｐ＝１８７＝Ｐ’×Ｐ’’＝（－１１）×（－１７）
と素因数分解できます.

「－１１」と「－１７」は「１１」と「１７」のことであると解釈します.

図式解法：Ｐ＝１８７の場合

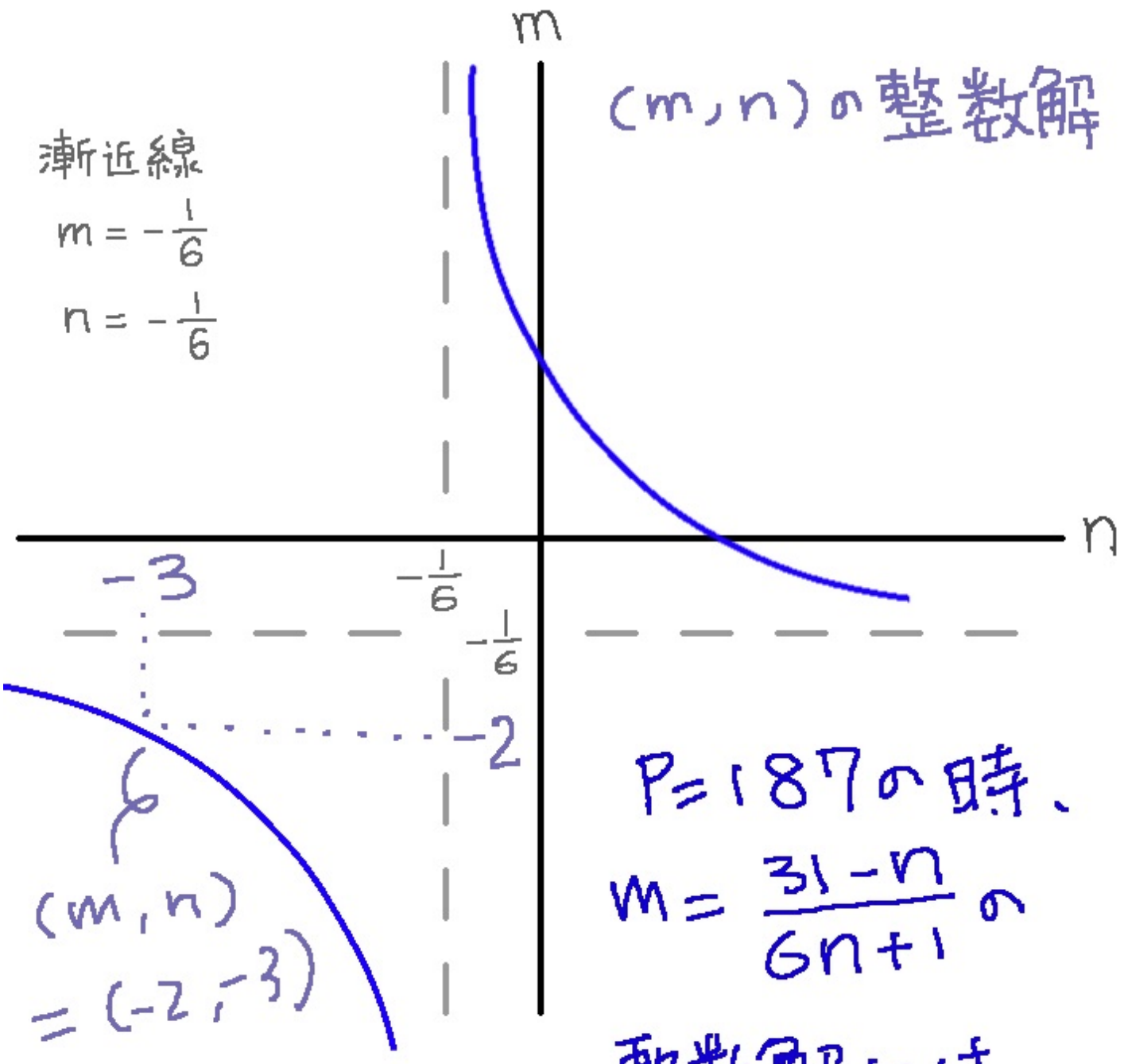
１８７＝３６ｍｎ＋６ｍ＋６ｎ＋１

この素数判定法定式を次のように変形します.

１８７－１＝３６ｍｎ＋６ｍ＋６ｎ
１８６＝３６ｍｎ＋６ｍ＋６ｎ
１８６÷６＝（３６ｍｎ＋６ｍ＋６ｎ）÷６
３１＝６ｍｎ＋ｍ＋ｎ
３１＝ｍ（６ｎ＋１）＋ｎ
３１－ｎ＝ｍ（６ｎ＋１）
（３１－ｎ）÷（６ｎ＋１）＝ｍ
ｍ＝（３１－ｎ）÷（６ｎ＋１）

縦軸をｍ、横軸をｎとして、上記の最後の式をグラフを書いて整数解を求めます.

グラフ：Ｐ＝１８７の場合



P=187の時、

$m=\frac{31-n}{6n+1}$ の

整数解には、

(-2,-3)があります。

$6m+1=-11$, $6n+1=-17$

負号無視して、 $187=11\times17$

となります。

計算例、Ｐ＝７４１の場合

７４１は６で割ると３余るので、６Ｎ＋３の形をしています．
従って、７４１は３の倍数です．
７４１＝３×２４７

それでは試しに、２４７が素数なのか合成数なのかの判定をしてみましょう．
２４７は６で割ると１余るので、６Ｎ＋１の形をしています．

そこで２４７を素数判定方程式のＰに代入しますと、
２４７＝３６ｍｎ＋６ｍ＋６ｎ＋１
となります．

この方程式のｍとｎの整数解を求めます．
ｍとｎに０以外の整数解があれば、Ｐは合成数であり、なければ素数となります．

この方程式を満たす整数解には、
（ｍ、ｎ）＝（２、３）
があります．従って、２４７は合成数です．

Ｐ’＝６ｍ＋１＝６×２＋１＝１３
Ｐ’’＝６ｎ＋１＝６×３＋１＝１９
つまり、
Ｐ＝２４７＝Ｐ’×Ｐ’’＝１３×１９
と素因数分解できます．

図式解法：Ｐ＝２４７の場合

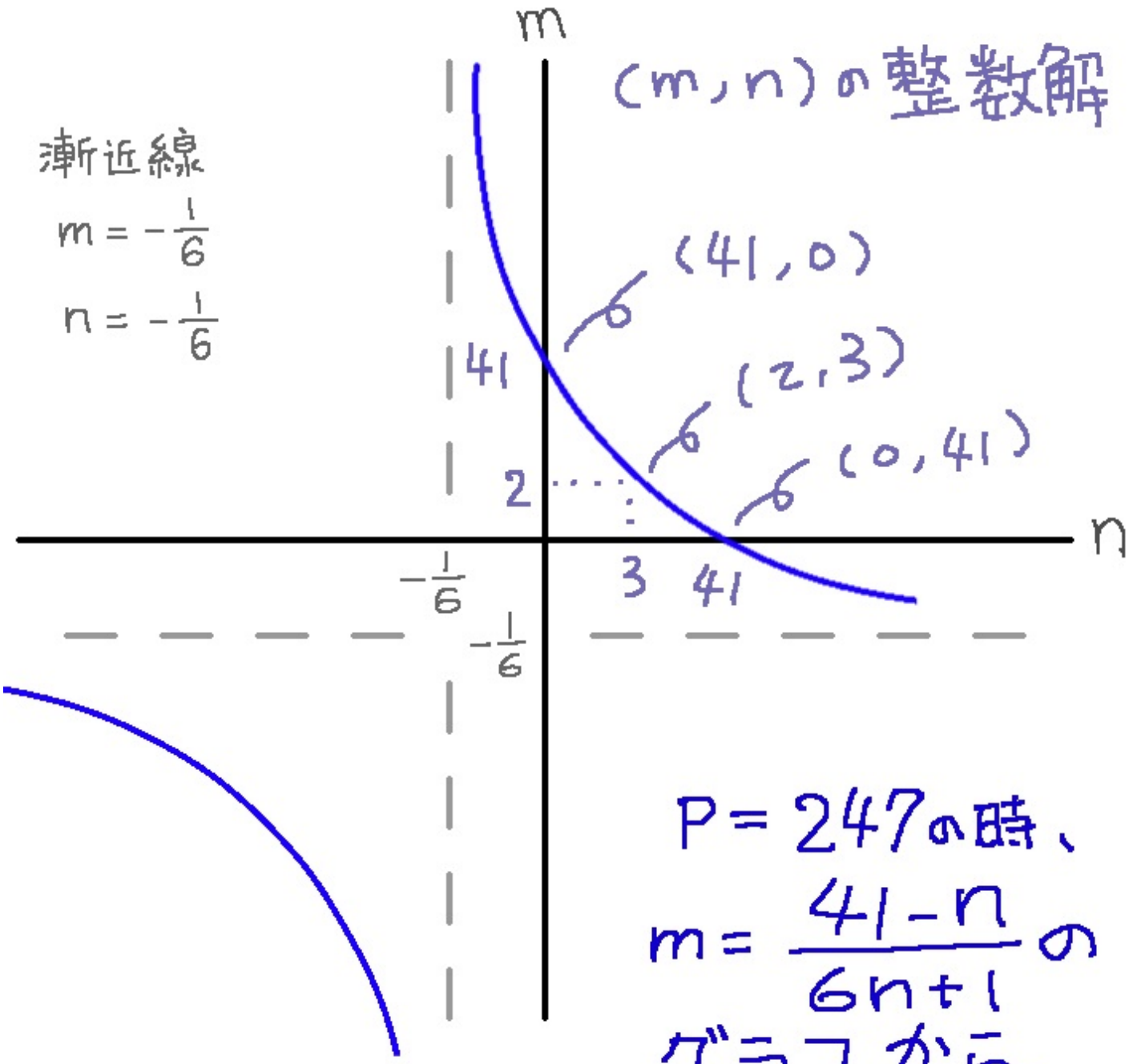
２４７＝３６ｍｎ＋６ｍ＋６ｎ＋１

この素数判定法定式を次のように変形します.

２４７－１＝３６ｍｎ＋６ｍ＋６ｎ
２４６＝３６ｍｎ＋６ｍ＋６ｎ
２４６÷６＝（３６ｍｎ＋６ｍ＋６ｎ）÷６
４１＝６ｍｎ＋ｍ＋ｎ
４１＝ｍ（６ｎ＋１）＋ｎ
４１－ｎ＝ｍ（６ｎ＋１）
（４１－ｎ）÷（６ｎ＋１）＝ｍ
ｍ＝（４１－ｎ）÷（６ｎ＋１）

縦軸をｍ、横軸をｎとして、上記の最後の式をグラフを書いて整数解を求めます.

グラフ：Ｐ＝２４７の場合



P=247の時、

$m=\frac{41-n}{6n+1}$ の

グラフから、

(m,n)=(2,3)を見つけます.

6m+1=13

6n+1=19 となりますので"

247=13×19 となります.

素数判定方程式の実用性について

素数判定方程式の整数解を求めるのは困難です.
ｍとｎをひとつひとつ調べることしか出来ないように思います.
理論的な考察の道具とは成り得ると思いますが、現状に於いて実用性はないと思います.
《了》

後書き

ＣＧ画像：
次の画像処理ソフトウエアを使用しました.

- ArtRage 3 Studio Pro　アンビエント社
- Photoshop Elements 10　アドビシステムズ株式会社

著者：
茜町春彦（あかねまちはるひこ）と申します.
2004年より活動を始めたフリーランスのライター＆イラストレーターです．独自のアイデア・考察を社会に提示することをミッションとし、平等で自由な世界の構築を目指して創作活動を行なっております．また、下記WEBサイトに於いても、デジタル作品を公開しております.

- YouTube　（動画共有サイト）
- Google+　（ソーシャルネットワークサービス）
- 楽天Kobo電子書籍ストア　（ネットショッピングサイト）
- はてなブログ　（WEBLOGサービス）
- Facebook ページ　（ソーシャルネットワークサービス）

その他：
製品名等はメーカー等の登録商標等です.

2017年9月9日発行

奥付

エッセイ（数学）『素数判定方程式』

http://p.booklog.jp/book/117130

著者：茜町春彦
著者プロフィール：http://p.booklog.jp/users/akaneharu/profile

感想はこちらのコメントへ
http://p.booklog.jp/book/117130

電子書籍プラットフォーム：パブー（http://p.booklog.jp/）
運営会社：株式会社トゥ・ディファクト