

$n^2 + 1$ 形式の素数

第三版 2013 年 3 月 30 日第 3 章追加

目次

第 1 章	$n^2 + 1$ 形式の素数	5
1.1	はじめに	5
1.2	$n^2 + 1$ 形式の素数	5
1.3	$k = 10a + x$	5
1.4	いろんな倍数	6
1.5	$k = Pa + x$	9
第 2 章	$n^2 + 1$ が合成数のとき	13
2.1	式の因数分解	13
2.2	合成数	13
2.3	判別式	17
第 3 章	2 つの連続する平方数の間に必ず素数が含まれることについて	21
3.1	n が偶数の時	21
3.2	n が奇数の時	23
3.3	演習	25

第 1 章

$n^2 + 1$ 形式の素数

1.1 はじめに

ふと、 $n^2 + 1$ 形式の素数が、無限にあることを証明せよという命題があることを知りました。では、逆に素数にならない場合を考えてみようではないかと思いました。これは、掲示板からまとめたメモです。編集、修正しました。なお、演算には、数式処理言語 maxima を使いました。

1.2 $n^2 + 1$ 形式の素数

$n^2 + 1$ 形式の素数 W において、いま、 $n = 2k + 1$ (つまり奇数) なら、
 $W = n^2 + 1 = (2k + 1)^2 + 1 = (4k^2 + 4k + 1) + 1 = 4k(k + 1) + 2 = 2\{2k(k + 1) + 1\}$
 であるから、 W は偶数になるので、 W が素数であるには、 n は偶数である。そこで、
 $n = 2k$ とおくと

$$W = n^2 + 1 = 4k^2 + 1$$

となる。

1.3 $k = 10a + x$

いま、 $k = 10a + x$ ($0 \leq x < 10$ の整数) (a は任意の整数) とする。つまり、 k を 10 の倍数表記をして、1 の位だけ x とする。ここで、 k はすべての自然数である。

x は 0 から 9 までなので、

```
(%i41) factor(4*(10*a+0)^2+1);
```

```
(%o41) 400 a2 + 1
```

```
(%i42) factor(4*(10*a+1)^2+1);
```

```
(%o42) 5 (80 a2 + 16 a + 1)
```

よって、 $x=1$ は、素数にならない。

```
(%i43) factor(4*(10*a+2)^2+1);
(%o43)          2
              400 a  + 160 a + 17
(%i44) factor(4*(10*a+3)^2+1);
(%o44)          2
              400 a  + 240 a + 37
(%i45) factor(4*(10*a+4)^2+1);
(%o45)          2
              5 (80 a  + 64 a + 13)
よって、x=4 は、素数にならない。
(%i46) factor(4*(10*a+5)^2+1);
(%o46)          2
              400 a  + 400 a + 101
(%i47) factor(4*(10*a+6)^2+1);
(%o47)          2
              5 (80 a  + 96 a + 29)
よって、x=6 は、素数にならない。
(%i48) factor(4*(10*a+7)^2+1);
(%o48)          2
              400 a  + 560 a + 197
(%i50) factor(4*(10*a+8)^2+1);
(%o50)          2
              400 a  + 640 a + 257
(%i49) factor(4*(10*a+9)^2+1);
(%o49)          2
              5 (80 a  + 144 a + 65)
よって、x=9 は、素数にならない。
```

したがって、 $x = 0, 2, 3, 5, 7, 8$ でないと素数になる可能性はない。

```
(%o41)          2
              400 a  + 1
(%o43)          2
              400 a  + 160 a + 17
(%o44)          2
              400 a  + 240 a + 37
(%o46)          2
              400 a  + 400 a + 101
(%o48)          2
              400 a  + 560 a + 197
(%o50)          2
              400 a  + 640 a + 257
```

素数なる可能性があるのは、この6通りです。ただし a は任意の自然数。

1.4 いろいろな倍数

$4k^2 + 1$ だから、 $k = p + 1$ とおくと

$$4k^2 + 1 = 4(p + 1)^2 + 1 = 4p^2 + 8p + 4 + 1 = 4p(p + 2) + 5$$

となります。したがって p が 5 の倍数なら $5\{4q(p+2)+1\}$ (ただし $p=5q$) となり、5 の倍数となります。

$k = 5a + x$ の場合 ($0 \leq x < 5$) の整数)

(%i1) factor(4*(5*a+0)^2+1);

(%o1) $100 a^2 + 1$

(%i2) factor(4*(5*a+1)^2+1);

(%o2) $5 (20 a^2 + 8 a + 1)$

よって、 $x=1$ は、素数にならない。

(%i3) factor(4*(5*a+2)^2+1);

(%o3) $100 a^2 + 80 a + 17$

(%i4) factor(4*(5*a+3)^2+1);

(%o4) $100 a^2 + 120 a + 37$

(%i5) factor(4*(5*a+4)^2+1);

(%o5) $5 (20 a^2 + 32 a + 13)$

よって、 $x=4$ は、素数にならない。

$k = 15a + x$ の場合 ($0 \leq x < 15$) の整数)

(%i7) factor(4*(15*a+0)^2+1);

(%o7) $900 a^2 + 1$

(%i8) factor(4*(15*a+1)^2+1);

(%o8) $5 (180 a^2 + 24 a + 1)$

よって、 $x=1$ は、素数にならない。

(%i9) factor(4*(15*a+2)^2+1);

(%o9) $900 a^2 + 240 a + 17$

(%i10) factor(4*(15*a+3)^2+1);

(%o10) $900 a^2 + 360 a + 37$

(%i11) factor(4*(15*a+4)^2+1);

(%o11) $5 (180 a^2 + 96 a + 13)$

よって、 $x=4$ は、素数にならない。

(%i12) factor(4*(15*a+5)^2+1);

(%o12) $900 a^2 + 600 a + 101$

(%i13) factor(4*(15*a+6)^2+1);

(%o13) $5 (180 a^2 + 144 a + 29)$

よって、 $x=6$ は、素数にならない。

(%i14) factor(4*(15*a+7)^2+1);

2

```
(%o14)          900 a  + 840 a + 197
(%i15) factor(4*(15*a+8)^2+1);
          2
(%o15)          900 a  + 960 a + 257
(%i16) factor(4*(15*a+9)^2+1);
          2
(%o16)          5 (180 a  + 216 a + 65)
よって、x=9 は、素数にならない。
(%i17) factor(4*(15*a+10)^2+1);
          2
(%o17)          900 a  + 1200 a + 401
(%i18) factor(4*(15*a+11)^2+1);
          2
(%o18)          5 (180 a  + 264 a + 97)
よって、x=11 は、素数にならない。
(%i19) factor(4*(15*a+12)^2+1);
          2
(%o19)          900 a  + 1440 a + 577
(%i20) factor(4*(15*a+13)^2+1);
          2
(%o20)          900 a  + 1560 a + 677
(%i21) factor(4*(15*a+14)^2+1);
          2
(%o21)          5 (180 a  + 336 a + 157)
よって、x=14 は、素数にならない。
```

ところが、

```
k=2a+x では、
(%i22) factor(4*(2*a+0)^2+1);
          2
(%o22)          16 a  + 1
(%i23) factor(4*(2*a+1)^2+1);
          2
(%o23)          16 a  + 16 a + 5

k=3a+x では、
(%i24) factor(4*(3*a+0)^2+1);
          2
(%o24)          36 a  + 1
(%i25) factor(4*(3*a+1)^2+1);
          2
(%o25)          36 a  + 24 a + 5
(%i26) factor(4*(3*a+2)^2+1);
          2
(%o26)          36 a  + 48 a + 17

k=4a+x では、
(%i27) factor(4*(4*a+0)^2+1);
```

2

```

(%o27)          2
              64 a  + 1
(%i28) factor(4*(4*a+1)^2+1);

              2
(%o28)          64 a  + 32 a + 5
(%i29) factor(4*(4*a+2)^2+1);

              2
(%o29)          64 a  + 64 a + 17
(%i30) factor(4*(4*a+3)^2+1);

              2
(%o30)          64 a  + 96 a + 37

k=6a+x では、
(%i31) factor(4*(6*a+0)^2+1);

              2
(%o31)          144 a  + 1
(%i32) factor(4*(6*a+1)^2+1);

              2
(%o32)          144 a  + 48 a + 5
(%i33) factor(4*(6*a+2)^2+1);

              2
(%o33)          144 a  + 96 a + 17
(%i34) factor(4*(6*a+3)^2+1);

              2
(%o34)          144 a  + 144 a + 37
(%i35) factor(4*(6*a+4)^2+1);

              2
(%o35)          144 a  + 192 a + 65
(%i36) factor(4*(6*a+5)^2+1);

              2
(%o36)          144 a  + 240 a + 101

```

どれも因数分解できませんね。

1.5 $k = Pa + x$

そこで、10の倍数表記でなくて、 P の倍数表記ではどうなるでしょうか。 $k = Pa + x$ とおくと

$$4k^2 + 1 = 4(Pa + x)^2 + 1$$

$$4k^2 + 1 = 4\{(Pa)^2 + 2Pax + x^2\} + 1$$

$$4k^2 + 1 = 4P(Pa^2 + 2ax) + 4x^2 + 1$$

であるから、約分できるのは、 $P = (4x^2 + 1)/b$ (ただし $0 \leq x < P$ 、 b は 1 以上の整数)の時だけです。

たとえば、 $P = 5$ なら、 $x = 1, b = 1$ 、 $x = 4, b = 13$

$$5 = (4x^2 + 1)/b \text{ (ただし、} 0 \leq x < 5)$$

$5b - (4x^2 + 1) = 0$ を満たす b, x です。

これまでをまとめると、

- $W = n^2 + 1$ 型の素数は、 n は偶数であり、であるから、
- $W = 4k^2 + 1$ (k は自然数) であり、
- $k = Pa + x$ なら (ただし $0 \leq x < P$ の整数、 a は任意の自然数)
- $P = (4x^2 + 1)/b$ (ただし $0 \leq x < P$ の整数、 b は 1 以上の整数)

という整数 P, x, b が存在すれば、それは素数になり得ない。

$4x^2 + 1 - Pb = 0$ において、 x を 0 から $P - 1$ まで変えて b について解けばよい。

素数にならないものを求めるには、 $P = 5$ なら、

```
(%i5) solve((4*0^2+1)-5*b=0,b);
(%o5) [b = -]
1
5

(%i6) solve((4*1^2+1)-5*b=0,b);
(%o6) [b = 1]

(%i7) solve((4*2^2+1)-5*b=0,b);
(%o7) [b = --]
17
5

(%i8) solve((4*3^2+1)-5*b=0,b);
(%o8) [b = --]
37
5

(%i9) solve((4*4^2+1)-5*b=0,b);
(%o9) [b = 13]
```

より、 $x = 1, b = 1, x = 4, b = 13$ が得られる。

また、 $(4x^2 + 1)/P = b$ であるから、 $4x^2 + 1$ は、 P の倍数でなければならない。

ところで、 $4x^2 + 1$ は $x = 1$ から 20 まで求めると

```
(%i40) 4*1^2+1;
(%o40) 5

(%i41) 4*2^2+1;
(%o41) 17

(%i42) 4*3^2+1;
(%o42) 37

(%i43) 4*4^2+1;
(%o43) 65

(%i44) 4*5^2+1;
(%o44) 101

(%i45) 4*6^2+1;
(%o45) 145

(%i46) 4*7^2+1;
(%o46) 197

(%i47) 4*8^2+1;
```

(%o47)	257
(%i48) $4 \cdot 9^2 + 1$;	
(%o48)	325
(%i49) $4 \cdot 10^2 + 1$;	
(%o49)	401
(%i50) $4 \cdot 11^2 + 1$;	
(%o50)	485
(%i51) $4 \cdot 12^2 + 1$;	
(%o51)	577
(%i52) $4 \cdot 13^2 + 1$;	
(%o52)	677
(%i53) $4 \cdot 14^2 + 1$;	
(%o53)	785
(%i55) $4 \cdot 15^2 + 1$;	
(%o55)	901
(%i56) $4 \cdot 16^2 + 1$;	
(%o56)	1025
(%i57) $4 \cdot 17^2 + 1$;	
(%o57)	1157
(%i58) $4 \cdot 18^2 + 1$;	
(%o58)	1297
(%i59) $4 \cdot 19^2 + 1$;	
(%o59)	1445
(%i60) $4 \cdot 20^2 + 1$;	
(%o60)	1601
(%i61)	
素因数分解してみると	
(%i20) <code>factor(4*1^2+1);</code>	
(%o20)	5
(%i21) <code>factor(4*2^2+1);</code>	
(%o21)	17
(%i22) <code>factor(4*3^2+1);</code>	
(%o22)	37
(%i23) <code>factor(4*4^2+1);</code>	
(%o23)	5 13
(%i24) <code>factor(4*5^2+1);</code>	
(%o24)	101
(%i25) <code>factor(4*6^2+1);</code>	
(%o25)	5 29
(%i26) <code>factor(4*7^2+1);</code>	
(%o26)	197
(%i27) <code>factor(4*8^2+1);</code>	
(%o27)	257
(%i28) <code>factor(4*9^2+1);</code>	
(%o28)	2
(%i29) <code>factor(4*10^2+1);</code>	
(%o29)	5 13
(%i30) <code>factor(4*11^2+1);</code>	
(%o30)	401
(%i31) <code>factor(4*12^2+1);</code>	
(%o31)	5 97

```

(%i31) factor(4*12^2+1);
(%o31)                                     577
(%i32) factor(4*13^2+1);
(%o32)                                     677
(%i33) factor(4*14^2+1);
(%o33)                                     5 157
(%i34) factor(4*15^2+1);
(%o34)                                     17 53
(%i35) factor(4*16^2+1);
(%o35)                                     2
(%i36) factor(4*17^2+1);
(%o36)                                     5 41
(%i37) factor(4*18^2+1);
(%o37)                                     13 89
(%i38) factor(4*19^2+1);
(%o38)                                     2
(%i39) factor(4*20^2+1);
(%o39)                                     5 17

```

となる。素因数分解できたものは、その因数もあるということである。

$4x^2 + 1$ が、 P の倍数でなければ、素数になる可能性は高い。

つまり、ここで、 P が決まると x はきまるから、 $4x^2 + 1$ が P の倍数でなければ、素数である可能性は失われない。

第2章

$n^2 + 1$ が合成数のとき

2.1 式の因数分解

$$f(x) = (x - a_0)(x - a_1)(x - a_2) \cdots (x - a_n) \quad (2.1)$$

において、 $f(a_0) = 0$ なので、 $f(x) = (x - a_0)g(x)$ また、 $f(a_1) = 0$ ならば、

$$f(x) = (x - a_0)(x - a_1)g'(x) \quad (2.2)$$

というふうに $f(x) = 0$ となる x の値で因数分解できるのでしたね。また、

$$f(0) = (-a_0)(-a_1)(-a_2) \cdots (-a_n) \quad (2.3)$$

であるから、 $a_0, a_1, a_2 \cdots a_n$ が自然数ならば、 $f(0)$ が自然数になるには、 a_0 から a_n は偶数個ですね。

ここで、 $a_0, a_1, a_2 \cdots a_n$ は、どれも等しくないとする。

2.2 合成数

いま、 $n^2 + 1$ が合成数で

$$n^2 + 1 = a_0 a_1 a_2 \cdots a_n \quad (2.4)$$

と表せるとすると、(ただし、 $a_0, a_1, a_2 \cdots a_n$ はどれも等しくないとする)

$$f(x) = (x - a_0)(x - a_1)(x - a_2) \cdots (x - a_n) \quad (2.5)$$

という関数 $f(x)$ を考え、 $x = 0$ として、式 2.4 から $n^2 + 1 = f(0)$ である。

$n^2 + 1$ が自然数であり、 $a_0 a_1 a_2 \cdots a_n$ は自然数であるから式 2.5 が、 $x = 0$ で、正であるという事は、 $a_0 a_1 a_2 \cdots a_n$ は偶数個でなければならない。

したがって、 $n^2 + 1$ は、偶数個の合成数だけを考えればいい。

さて、

$$n^2 + 1 - f(a_0) = n^2 + 1 - (a_0 - a_0)(a_0 - a_1)(a_0 - a_2) \cdots (a_0 - a_n) = n^2 + 1$$

であるから、例えば、式 2.5 が、2項として

$$\begin{aligned} n^2 + 1 &= (x - a_0)(x - a_1) \\ n^2 + 1 - a_0a_1 &= x^2 - (a_0 + a_1)x \end{aligned}$$

ここで、 $n^2 + 1 = a_0a_1$ であるから、

$$\begin{aligned} x^2 - (a_0 + a_1)x &= 0 \\ x - (a_0 + a_1) &= 0 \\ x &= a_0 + a_1 \end{aligned}$$

また、 $n^2 + 1 = a_0a_1$ であるから、

$$\begin{aligned} n^2 + 1 &= (x - a_1)a_1 \\ \frac{n^2 + 1}{a_1} &= x - a_1 \\ \frac{n^2 + 1}{a_1} + a_1 &= x \\ \frac{n^2 + 1 + a_1^2}{a_1} &= x \end{aligned}$$

となる。

2.2.1 演習 1

ここで、 $n=8$ なら、

$$\begin{aligned} \frac{8^2 + 1 + a_1^2}{a_1} &= x \\ \frac{65 + a_1^2}{a_1} &= x \end{aligned}$$

そこで、 $x = 1$ から増やしながらか a_1 について解くと、

```
(%i1) solve((65+a^2)/a=1,a);
      sqrt(259) %i - 1      sqrt(259) %i + 1
(%o1)      [a = - -----, a = -----]
              2              2

(%i2) solve((65+a^2)/a=2,a);
      [a = 1 - 8 %i, a = 8 %i + 1]
(%o2)
(%i3) solve((65+a^2)/a=3,a);
      sqrt(251) %i - 3      sqrt(251) %i + 3
(%o3)      [a = - -----, a = -----]
              2              2

(%i4) solve((65+a^2)/a=4,a);
```

```

(%o4) [a = 2 - sqrt(61) %i, a = sqrt(61) %i + 2]
(%i5) solve((65+a^2)/a=5,a);
(%o5) [a = -  $\frac{\sqrt{235} \%i - 5}{2}$ , a =  $\frac{\sqrt{235} \%i + 5}{2}$ ]
(%i6) solve((65+a^2)/a=6,a);
(%o6) [a = 3 - 2 sqrt(14) %i, a = 2 sqrt(14) %i + 3]
(%i7) solve((65+a^2)/a=7,a);
(%o7) [a = -  $\frac{\sqrt{211} \%i - 7}{2}$ , a =  $\frac{\sqrt{211} \%i + 7}{2}$ ]
(%i8) solve((65+a^2)/a=8,a);
(%o8) [a = 4 - 7 %i, a = 7 %i + 4]
(%i9) solve((65+a^2)/a=9,a);
(%o9) [a = -  $\frac{\sqrt{179} \%i - 9}{2}$ , a =  $\frac{\sqrt{179} \%i + 9}{2}$ ]
(%i10) solve((65+a^2)/a=10,a);
(%o10) [a = 5 - 2 sqrt(10) %i, a = 2 sqrt(10) %i + 5]
(%i11) solve((65+a^2)/a=11,a);
(%o11) [a = -  $\frac{\sqrt{139} \%i - 11}{2}$ , a =  $\frac{\sqrt{139} \%i + 11}{2}$ ]
(%i12) solve((65+a^2)/a=12,a);
(%o12) [a = 6 - sqrt(29) %i, a = sqrt(29) %i + 6]
(%i13) solve((65+a^2)/a=13,a);
(%o13) [a = -  $\frac{\sqrt{91} \%i - 13}{2}$ , a =  $\frac{\sqrt{91} \%i + 13}{2}$ ]
(%i14) solve((65+a^2)/a=14,a);
(%o14) [a = 7 - 4 %i, a = 4 %i + 7]
(%i15) solve((65+a^2)/a=15,a);
(%o15) [a = -  $\frac{\sqrt{35} \%i - 15}{2}$ , a =  $\frac{\sqrt{35} \%i + 15}{2}$ ]
(%i16) solve((65+a^2)/a=16,a);
(%o16) [a = 8 - %i, a = %i + 8]
(%i17) solve((65+a^2)/a=17,a);
(%o17) [a = -  $\frac{\sqrt{29} - 17}{2}$ , a =  $\frac{\sqrt{29} + 17}{2}$ ]
(%i18) solve((65+a^2)/a=18,a);
(%o18) [a = 13, a = 5]
(%i19)

```

より、 $a_1 = 13, 5$ が得られる。つまり、 a_0, a_1 は $13, 5$ である。

ために、 $8^2 + 1 = 65 = 13 \times 5$ であっている。

2.2.2 演習 2

$$\frac{n^2 + 1 + a_1^2}{a_1} = x \quad (2.6)$$

において、 $n^2 + 1$ は奇数であるから、 $n^2 + 1 = a_0 a_1$ より、 a_0, a_1 も奇数である。

したがって、分子は偶数になり分母が奇数だから、 x は自然数より、 x は偶数でなければならない。

よって、 $x = 2$ から 2 ずつ増やせばよい。

そこで、 $n = 12$ の時 $x = 2$ から 2 ずつ増やしてゆくと

```
(%i106) solve((145+a^2)/a=34,a);
(%o106) [a = 5, a = 29]
```

より a_0, a_1 は 5, 29 である。 $12^2 + 1 = 145 = 5 \times 29$ であっている。では、 $n = 18$ の時

```
(%i109) factor(18^2+1);
(%o109) 2
5 13
```

これは、どうなる？ 3 個だぞ。でも 25, 13 とも言える。これより、 $x = 2$ から 2 ずつ増やしてゆくと、

```
(%i110) solve((325+a^2)/a=2,a);
(%o110) [a = 1 - 18 %i, a = 18 %i + 1]
(%i111) solve((325+a^2)/a=4,a);
(%o111) [a = 2 - sqrt(321) %i, a = sqrt(321) %i + 2]
(%i112) solve((325+a^2)/a=6,a);
(%o112) [a = 3 - 2 sqrt(79) %i, a = 2 sqrt(79) %i + 3]
(%i113) solve((325+a^2)/a=8,a);
(%o113) [a = 4 - sqrt(309) %i, a = sqrt(309) %i + 4]
(%i114) solve((325+a^2)/a=10,a);
(%o114) [a = 5 - 10 sqrt(3) %i, a = 10 sqrt(3) %i + 5]
(%i115) solve((325+a^2)/a=12,a);
(%o115) [a = 6 - 17 %i, a = 17 %i + 6]
(%i116) solve((325+a^2)/a=14,a);
(%o116) [a = 7 - 2 sqrt(69) %i, a = 2 sqrt(69) %i + 7]
(%i117) solve((325+a^2)/a=16,a);
(%o117) [a = 8 - 3 sqrt(29) %i, a = 3 sqrt(29) %i + 8]
(%i118) solve((325+a^2)/a=18,a);
(%o118) [a = 9 - 2 sqrt(61) %i, a = 2 sqrt(61) %i + 9]
(%i119) solve((325+a^2)/a=20,a);
(%o119) [a = 10 - 15 %i, a = 15 %i + 10]
(%i120) solve((325+a^2)/a=22,a);
(%o120) [a = 11 - 2 sqrt(51) %i, a = 2 sqrt(51) %i + 11]
(%i121) solve((325+a^2)/a=24,a);
(%o121) [a = 12 - sqrt(181) %i, a = sqrt(181) %i + 12]
(%i122) solve((325+a^2)/a=26,a);
```

```
(%o122) [a = 13 - 2 sqrt(39) %i, a = 2 sqrt(39) %i + 13]
(%i123) solve((325+a^2)/a=28,a);
(%o123) [a = 14 - sqrt(129) %i, a = sqrt(129) %i + 14]
(%i124) solve((325+a^2)/a=30,a);
(%o124) [a = 15 - 10 %i, a = 10 %i + 15]
(%i125) solve((325+a^2)/a=32,a);
(%o125) [a = 16 - sqrt(69) %i, a = sqrt(69) %i + 16]
(%i126) solve((325+a^2)/a=34,a);
(%o126) [a = 17 - 6 %i, a = 6 %i + 17]
(%i127) solve((325+a^2)/a=36,a);
(%o127) [a = 18 - %i, a = %i + 18]
(%i128) solve((325+a^2)/a=38,a);
(%o128) [a = 25, a = 13]
(%i129)
```

より、 a_0, a_1 は 25, 13 である。 $18^2 + 1 = 325 = 25 \times 13$ であっている。

2.3 判別式

$$\frac{n^2 + 1 + a_1^2}{a_1} = x$$

において、 $a_1 = y, x = 2p$ とすると、

$$\begin{aligned} n^2 + 1 + y^2 &= 2py \\ y^2 - 2py + n^2 + 1 &= 0 \end{aligned}$$

となる。2 次方程式の解の公式から

$$\begin{aligned} y &= \frac{-(-2p) \pm \sqrt{(-2p)^2 - 4(n^2 + 1)}}{2} \\ y &= p \pm \sqrt{p^2 - (n^2 + 1)} \end{aligned}$$

となる。 y は自然数なので、 $y = p - \sqrt{p^2 - (n^2 + 1)} > 0$ でなければならない。

また、 $m = \sqrt{p^2 - (n^2 + 1)}$ とすると、 m も自然数でなければならない。

よって $m^2 = p^2 - n^2 - 1$ でなければならない。

また、 m が自然数であるから $n < p$ でなければならない。

2.3.1 演習 1

そこで、 $p = n + q$ とおくと

$$\begin{aligned} m^2 &= p^2 - (n^2 + 1) \\ m^2 &= (n + q)^2 - n^2 - 1 \end{aligned}$$

$$m^2 = n^2 + 2nq + q^2 - n^2 - 1$$

$$m^2 = 2nq + q^2 - 1$$

ために、 $n = 8$ なら $p = n + 1$ として

$$m^2 = 2 \times 8 \times 1 + 1^2 - 1$$

$$m^2 = 16 + 1 - 1$$

$$m^2 = 16$$

よって、 $m = 4$ であり、

$$y = (n + 1) \pm 4$$

$$y = 8 + 1 \pm 4$$

$$y = 9 \pm 4$$

より、 $y = 13, 5$ をえる。ゆえに、 a_0, a_1 は $13, 5$ である。

2.3.2 演習 2

同じようにして、 $n = 12$ ならば、 $p = n + 1$ として

$$m^2 = 2 \times 12 \times 1 + 1^2 - 1$$

$$m^2 = 24$$

より、自然数の解はない。そこで、 $p = n + 2$ として

$$m^2 = 2 \times 12 \times 2 + 2^2 - 1$$

$$m^2 = 48 + 4 - 1$$

$$m^2 = 51$$

より、自然数の解はない。そこで、 $p = n + 3$ として

$$m^2 = 2 \times 12 \times 3 + 3^2 - 1$$

$$m^2 = 72 + 9 - 1$$

$$m^2 = 80$$

より、自然数の解はない。そこで、 $p = n + 4$ として

$$m^2 = 2 \times 12 \times 4 + 4^2 - 1$$

$$m^2 = 96 + 16 - 1$$

$$m^2 = 111$$

より、自然数の解はない。そこで、 $p = n + 5$ として

$$m^2 = 2 \times 12 \times 5 + 5^2 - 1$$

$$m^2 = 120 + 25 - 1$$

$$m^2 = 144$$

よって、 $m = 12$ であり、

$$y = (n + 5) \pm 12$$

$$y = 17 \pm 12$$

より、 $y = 29, 5$ をえる。ゆえに、 a_0, a_1 は $29, 5$ である。

第3章

2つの連続する平方数の間に必ず素数が含まれることについて

さて、2つの連続する平方数の間に必ず素数が含まれることについて考えてみましょう。そこで、2つの連続する平方数の間がすべて、合成数であるとしたら、素数は含まれないこととなります。つまり、2つの連続する平方数の間が、すべて合成数で埋められなければ、素数が入ることになりますね。

3.1 n が偶数の時

n が偶数の時、 $n+2$ までがすべて合成数ならば、奇数 $n^2 + 1$ から奇数 $(n+2)^2 - 1$ まで、2つつ増えるので奇数は $n^2 + 1 + 2k$ と表せます。偶数はすべて合成数であるから考える必要はありません。すると判別式は、

$$\frac{n^2 + 1 + 2k + a_1^2}{a_1} = x$$

において、 $a_1 = y, x = 2p$ とすると、

$$\begin{aligned} n^2 + 1 + 2k + y^2 &= 2py \\ y^2 - 2py + n^2 + 1 + 2k &= 0 \end{aligned}$$

となる。2次方程式の解の公式から

$$\begin{aligned} y &= \frac{-(-2p) \pm \sqrt{(-2p)^2 - 4(n^2 + 1 + 2k)}}{2} \\ y &= p \pm \sqrt{p^2 - (n^2 + 1 + 2k)} \end{aligned}$$

となる。 y は自然数なので、 $y = p - \sqrt{p^2 - (n^2 + 1 + 2k)} > 0$ でなければならない。

また、 $m = \sqrt{p^2 - (n^2 + 1 + 2k)}$ とすると、 m も自然数でなければならない。

よって $m^2 = p^2 - n^2 - 1 - 2k$ でなければならない。

また、 m が自然数であるから $n < p$ でなければならない。よって、

$$n^2 + 1 + 2k = p^2 - m^2 \quad (\text{ただし } m \neq 0) \quad (3.1)$$

である。

ここで、 $k = 0$ ならば、

$$n^2 + 1 = p_0^2 - m_0^2 \quad (3.2)$$

$k = 1$ ならば、

$$n^2 + 1 + 2 = p_1^2 - m_1^2 \quad (3.3)$$

また $k = 2$ ならば、

$$n^2 + 1 + 4 = p_2^2 - m_2^2 \quad (3.4)$$

$k = 3$ ならば、

$$n^2 + 1 + 6 = p_3^2 - m_3^2 \quad (3.5)$$

いま、式 3.3 から式 3.2 を引くと

$$\begin{aligned} n^2 + 1 + 2 - (n^2 + 1) &= p_1^2 - m_1^2 - p_0^2 - m_0^2 \\ 2 &= p_1^2 - m_1^2 - p_0^2 - m_0^2 \end{aligned} \quad (3.6)$$

同じようにして式 3.4 から式 3.3 を引くと

$$\begin{aligned} n^2 + 1 + 4 - (n^2 + 1 + 2) &= p_2^2 - m_2^2 - p_1^2 - m_1^2 \\ 2 &= p_2^2 - m_2^2 - p_1^2 - m_1^2 \end{aligned} \quad (3.7)$$

そこで、式 3.7 から式 3.6 を引くと

$$\begin{aligned} 2 - 2 &= p_2^2 - m_2^2 - p_1^2 - m_1^2 - \{p_1^2 - m_1^2 - p_0^2 - m_0^2\} \\ 2(p_1^2 - m_1^2) &= p_2^2 - m_2^2 + p_0^2 - m_0^2 \end{aligned}$$

つまり、合成数は、前後の合成数の和で表せる。いま、 $k = w$ ならば、

$$2(p_{w+1}^2 - m_{w+1}^2) = p_{w+2}^2 - m_{w+2}^2 + p_w^2 - m_w^2 \quad (3.8)$$

である。したがって、 $n^2 + 1$ から $(n+2)^2 - 1$ までこれが成り立たねばならない。

$$(n+2)^2 - 1 = (n+2)^2 - 1^2$$

であり、 $p = (n+2)$ 、 $m = 1$ であり、式 3.1 を満足している。

$$n^2 + 1 = p_0^2 - m_0^2$$

であるから、両端が式 3.8 を満足するから、あいだはすべて式 3.8 成立つ。

また、 n^2 と $(n+1)^2$ の間では 2 乗数がないので、 m は 0 にならない。

ところが、 $(n+1)^2$ は奇数であり、また、2乗数であるから、

$$(n+1)^2 = p_v^2 - m_v^2$$

$$(n+1)^2 = (p_v + m_v)(p_v - m_v)$$

ではありえない。

また、式 2.4 より、 $m \neq 0$ である。^{*1}

$$(n+1)^2 = p_v^2 - m_v^2 \quad (\text{ただし } m \neq 0) \quad (3.9)$$

したがって、式 3.9 とはならない。式 3.1 では表せない。すると片方の端で式 3.9 が成り立たないので、すべて式 3.8 成り立たなくなり、 $n^2 + 1$ から $(n+1)^2$ の間で、式 3.8 は成り立たない。ゆえに、 n が偶数なら、 $n^2 + 1$ から $(n+1)^2$ まで合成数で埋めることはできない。

3.2 n が奇数の時

n が奇数の時、 $n+2$ までがすべて合成数ならば、奇数 $n^2 + 2$ から奇数 $(n+2)^2 - 2$ まで、2つづ増えるので奇数は $n^2 + 2 + 2k$ と表せます。偶数はすべて合成数ですから、考える必要はありません。すると判別式は、

$$\frac{n^2 + 2 + 2k + a_1^2}{a_1} = x$$

において、 $a_1 = y, x = 2p$ とすると、

$$n^2 + 2 + 2k + y^2 = 2py$$

$$y^2 - 2py + n^2 + 2 + 2k = 0$$

となる。2次方程式の解の公式から

$$y = \frac{-(-2p) \pm \sqrt{(-2p)^2 - 4(n^2 + 2 + 2k)}}{2}$$

$$y = p \pm \sqrt{p^2 - (n^2 + 2 + 2k)}$$

となる。 y は自然数なので、 $y = p - \sqrt{p^2 - (n^2 + 2 + 2k)} > 0$ でなければならない。

また、 $m = \sqrt{p^2 - (n^2 + 2 + 2k)}$ とすると、 m も自然数でなければならない。

よって $m^2 = p^2 - n^2 - 2 - 2k$ でなければならない。

また、 m が自然数であるから $n < p$ でなければならない。よって、

$$n^2 + 2 + 2k = p^2 - m^2 \quad (\text{ただし } m \neq 0) \quad (3.10)$$

^{*1} ただし、 $a_0, a_1, a_2 \dots a_n$ はどれも等しくないとする

である。

ここで、 $k = 0$ ならば、

$$n^2 + 2 = p_0^2 - m_0^2 \quad (3.11)$$

$k = 1$ ならば、

$$n^2 + 2 + 2 = p_1^2 - m_1^2 \quad (3.12)$$

また $k = 2$ ならば、

$$n^2 + 2 + 4 = p_2^2 - m_2^2 \quad (3.13)$$

$k = 3$ ならば、

$$n^2 + 2 + 6 = p_3^2 - m_3^2 \quad (3.14)$$

いま、式 3.12 から式 3.11 を引くと

$$\begin{aligned} n^2 + 2 + 2 - (n^2 + 2) &= p_1^2 - m_1^2 - p_0^2 - m_0^2 \\ 2 &= p_1^2 - m_1^2 - p_0^2 - m_0^2 \end{aligned} \quad (3.15)$$

同じようにして式 3.13 から式 3.12 を引くと

$$\begin{aligned} n^2 + 2 + 4 - (n^2 + 2 + 2) &= p_2^2 - m_2^2 - p_1^2 - m_1^2 \\ 2 &= p_2^2 - m_2^2 - p_1^2 - m_1^2 \end{aligned} \quad (3.16)$$

そこで、式 3.16 から式 3.15 を引くと

$$\begin{aligned} 2 - 2 &= p_2^2 - m_2^2 - p_1^2 - m_1^2 - \{p_1^2 - m_1^2 - p_0^2 - m_0^2\} \\ 2(p_1^2 - m_1^2) &= p_2^2 - m_2^2 + p_0^2 - m_0^2 \end{aligned}$$

つまり、合成数は、前後の合成数の和で表せる。いま、 $k = w$ ならば、

$$2(p_{w+1}^2 - m_{w+1}^2) = p_{w+2}^2 - m_{w+2}^2 + p_w^2 - m_w^2 \quad (3.17)$$

である。したがって、奇数 $n^2 + 2$ から奇数 $(n + 2)^2 - 2$ までこれが成り立たねばならない。

また、 n^2 と $(n + 1)^2$ の間では 2 乗数がないので、 m は 0 にならない。

ところが、 $(n + 1)^2$ が偶数であるので、

$$\begin{aligned} (n + 1)^2 - 1 &= p_v^2 - m_v^2 \\ (n + 1)^2 - 1 &= (p_v + m_v)(p_v - m_v) \end{aligned}$$

ゆえに $p_v = n + 1$ 、 $m_v = 1$ である。

では、先頭の n^2 は、

$$n^2 = p_v^2 - m_v^2 \text{ (ただし } m \neq 0 \text{)} \quad (3.18)$$

また、式 2.4 より、 $m \neq 0$ である。^{*2}

したがって、式 3.18 とはならない。すると片方の端で、式 3.18 が成り立たないので、 n^2 から $(n+1)^2 - 1$ の間ですべて式 3.17 成り立たなくなってしまう、 n^2 から $(n+1)^2 - 1$ の間で、式 3.17 は成り立たない。ゆえに、 n が奇数なら、 n^2 から $(n+1)^2$ まで合成数で埋めることはできない。

よって、連続する 2 平方数の間を合成数で埋めることができないので、必ず奇数が含まれる。

3.3 演習

```
(%i1) factor(14^2+1);
(%o1) 197
(%i2) factor(14^2+3);
(%o2) 199
(%i3) factor(14^2+5);
(%o3) 3 67 =(35+32)(35-32)
(%i4) factor(14^2+7);
(%o4) 7 29 =(18+11)(18-11)
(%i5) factor(14^2+9);
(%o5) 5 41=(23+18)(23-18)
(%i6) factor(14^2+11);
(%o6) 2
3 23=9 23=(16+7)(16-7)
(%i9) factor(14^2+13);
(%o9) 11 19=(15+4)(15-4)
(%i10) factor(14^2+15);
(%o10) 211
(%i11) factor(14^2+17);
(%o11) 3 71=(37+34)(37-34)
(%i12) factor(14^2+19);
(%o12) 5 43=(24+19)(24-19)
(%i13) factor(14^2+21);
(%o13) 7 31=(19+12)(19-12)
(%i14) factor(14^2+23);
(%o14) 3 73=(38+35)(38-35)
(%i15) factor(14^2+25);
(%o15) 13 17=(15+2)(15-2)

(%i16) factor(15^2+2);
(%o16) 227
(%i17) factor(15^2+4);
(%o17) 229
(%i18) factor(15^2+6);
(%o18) 3 7 11=21 11=(16+5)(16-5)
(%i19) factor(15^2+8);
```

^{*2} ただし、 $a_0, a_1, a_2 \dots a_n$ はどれも等しくないとする

```

(%o19)                                     233
(%i20) factor(15^2+10);
(%o20)                                     5 47=(26+21)(26-21)
(%i21) factor(15^2+12);
(%o21)                                     3 79=(41+38)(41-38)
(%i22) factor(15^2+14);
(%o22)                                     239
(%i23) factor(15^2+16);
(%o23)                                     241
(%i24) factor(15^2+18);
(%o24)                                     5
3 27=(18+9)(18-9)
3 81=(42+39)(42-39)
(%i25) factor(15^2+20);
(%o25)                                     2
5 7 49=(27+22)(27-22)
7 35=(21+14)(21-14)
(%i26) factor(15^2+22);
(%o26)                                     13 19=(16+3)(16-3)
(%i27) factor(15^2+24);
(%o27)                                     3 83=(43+40)(43-40)
(%i28) factor(15^2+26);
(%o28)                                     251
(%i29) factor(15^2+28);
(%o29)                                     11 23=(17+6)(17-6)
(%i30) factor(15^2+30);
(%o30)                                     3 5 17=15 17=(16+1)(16-1)
=5 51=(28+23)(28-23)
=3 85=(44+41)(44-41)

```