

素数の判別方法-エラトステネスの篩の特殊形-

八野 正

1997年9月14日

0.1 素数

素数は、 $6n \pm 1$ が、2 と 3 の倍数を除いた一般形式の候補式である。

$$(5, 7), (11, 13), (17, 19), (23, 25), (29, 31), (35, 37), (41, 43), (47, 49), (53, 55),$$

$$(59, 61), (65, 67), (71, 73), (77, 79), (83, 85), (89, 91), (95, 97), (101, 103), (107, 109),$$

$$(113, 115), (119, 121), (125, 127), (131, 133), (137, 139), (143, 145), (149, 151),$$

これは、一部である。5 から初めて 2 と 4 を交互に加えた数列である。

$$25 = 5 + 2 + (4 + 2) + (4 + 2) + (4 + 2) \quad (0.1)$$

$$35 = 25 + 4 + (2 + 4) \quad (0.2)$$

$$55 = 35 + 2 + (4 + 2) + (4 + 2) + (4 + 2) \quad (0.3)$$

$$65 = 55 + 4 + (2 + 4) \quad (0.4)$$

$$85 = 65 + 2 + (4 + 2) + (4 + 2) + (4 + 2) \quad (0.5)$$

$$95 = 85 + 4 + (2 + 4) \quad (0.6)$$

より、5からはじめて7こめすなわち、

$$25 = 5 + \{2 + (4 + 2) \times 3\} = 5 + (2 + 6 \times 3) \quad (0.7)$$

とそこからはじめて、3こめ

$$35 = 25 + \{4 + (4 + 2)\} = 25 + (4 + 6) \quad (0.8)$$

となり、また 35 の次の 37 は、 $35 + 2$ から始まるので、7こめ、3こめの繰り返しとなり、今後 5 の倍数は、これをもってすべて排除される。

同じようにして、

$$35 = 7 + 4 + (2 + 4) + (2 + 4) + (2 + 4) + (2 + 4) = 7 + 28 = 7 + (4 + 6 \times 4) \quad (0.9)$$

$$49 = 35 + 2 + (4 + 2) + (4 + 2) = 35 + 14 = 35 + (2 + 6 \times 2) \quad (0.10)$$

となり、今後 7 の倍数は、これをもってすべて排除される。

$$55 = 11 + 2 + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2)$$

$$= 11 + 44 = 11 + (2 + 6 \times 7)$$

$$77 = 55 + 4 + (2 + 4) + (2 + 4) + (2 + 4) = 55 + 22 = 55 + (4 + 6 \times 3) \quad (0.11)$$

となり、今後 11 の倍数は、これをもってすべて排除される。

$$65 = 13 + 4 + (2 + 4) + (2 + 4) + (2 + 4) + (2 + 4) + (2 + 4) + (2 + 4) + (2 + 4) + (2 + 4)$$

$$= 13 + 52 = 13 + (4 + 6 \times 8)$$

$$91 = 65 + 2 + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) = 65 + 26 = 65 + (2 + 6 \times 4) \quad (0.12)$$

となり、今後 13 の倍数は、これをもってすべて排除される。

$$\begin{aligned} 85 &= 17 + 2 + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) + (4 + 2) \\ &= 17 + 68 = 17 + (2 + 6 \times 11) \end{aligned}$$

$$119 = 85 + 4 + (2 + 4) + (2 + 4) + (2 + 4) + (2 + 4) + (2 + 4) = 85 + 34 = 85 + (4 + 6 \times 5) \quad (0.13)$$

となり、今後 17 の倍数は、これをもってすべて排除される。

このようにある繰り返しが生じる。これをエラトステネスの篩の特殊形と呼ぶとする。

0.2 素数のエラトステネスの篩の特殊形の一般型

そこで、

$$6n - 1 + \frac{2 + 6m}{6n - 1} = p \quad (0.14)$$

となる整数 p, m が存在するとき、それは、 $6n - 1$ の倍数である。また、

$$6n + 1 + \frac{4 + 6k}{6n + 1} = v \quad (0.15)$$

となる整数 v, k が存在するとき、それは、 $6n + 1$ の倍数である。

0.2.1 素数のエラトステネスの篩の特殊形の一般型 $6n - 1$

$$\frac{2 + 6m}{6n - 1} = p - (6n - 1) = q (q \text{ は整数}) \quad (0.16)$$

$$\frac{2 + 6m}{6n - 1} = q \quad (0.17)$$

となる。そこで、

$$\frac{2 + 6m}{6n - 1} = q \quad (0.18)$$

を展開して整理すると、

$$2 + 6m = 6nq - q \quad (0.19)$$

$$6m = 6nq - q - 2 \quad (0.20)$$

が得られる。

$$m = nq - \frac{q + 2}{6} \quad (0.21)$$

ここで、 m は整数より、

$$6z = q + 2 \quad (0.22)$$

となる z が存在する。

よって、

$$\frac{6m+2}{6n-1} = q \quad (0.23)$$

より、

$$6m+2 = (6n-1)q \quad (0.24)$$

$$6m+2 = (6n-1)(6z-2) \quad (0.25)$$

したがって、最初の $6n-1$ の次は、

$$6n-1, 6n-1+(6m+2), \quad (0.26)$$

$$6n-1, 6n-1+(6n-1)(6z-2), \quad (0.27)$$

さらにその次は、前の数から $4+6k$ すすんだところにあるので、 q を作り出したように

$$6n-1+(6n-1)(6z-2) + \frac{4+6k}{6n-1} = u \quad (0.28)$$

となる u, k が存在する。これより、 v を切り出す。

$$\frac{4+6k}{6n-1} = v \quad (0.29)$$

よって、 q から z を作り出したように、 y が次のように作り出せる。

$$6y = v + 4 \quad (0.30)$$

であるから、

$$4+6k = (6n-1)v \quad (0.31)$$

$$4+6k = (6n-1)(6y-4) \quad (0.32)$$

であるから、最初の $6n-1$ の次とその次は、

$$6n-1, 6n-1+(6m+2), 6n-1+(6m+2)+(4+6k) \quad (0.33)$$

したがって、エラトステネス篩の特殊形は、次のように完成される。

$$(6n-1), \quad (0.34)$$

$$(6n-1) + (6n-1)(6z-2), \quad (0.35)$$

$$(6n-1) + (6n-1)(6z-2) + (6n-1)(6y-4), \quad (0.36)$$

$$(6n-1) + (6n-1)(6z-2) + (6n-1)(6y-4) + (6n-1)(6z-2), \quad (0.37)$$

$$(6n-1) + (6n-1)(6z-2) + (6n-1)(6y-4) + (6n-1)(6z-2) + (6n-1)(6y-4), \quad (0.38)$$

したがって、ある $6n-1$ 型の素数の倍数の一般形は

$$(6n-1) \quad (0.39)$$

以下の2つは、交互に現れる。1つめは、

$$(6n-1)[1+g\{(6z-2)+(6y-4)\}+(6z-2)](g\text{は自然数}) \quad (0.40)$$

$$(6n-1)\{1+6g(z+y-1)+6z-2\}(g\text{は自然数}) \quad (0.41)$$

$$(6n-1)(6a-1)\{\text{但し } a = g(z+y-1)+z\} \quad (0.42)$$

2つめは、

$$(6n-1)[1+g\{(6z-2)+(6y-4)\}+(6z-2)+(6y-4)](g\text{は自然数}) \quad (0.43)$$

$$(6n-1)\{1+6g(z+y-1)+6(z+y-1)\}(g\text{は自然数}) \quad (0.44)$$

$$(6n-1)(6b+1)\{\text{但し } b = (g+1)(z+y-1)\} \quad (0.45)$$

0.2.2 素数のエラトステネスの篩の特殊形の一般型 $6n+1$

また、 $6n+1$ 型の数は、

$$\frac{4+6m}{6n+1} = q \quad (0.46)$$

$$4+6m = 6nq + q \quad (0.47)$$

$$6m = 6nq + q - 4 \quad (0.48)$$

となり、

$$m = nq + \frac{q-4}{6} \quad (0.49)$$

ここで、 m は整数より、

$$6z = q - 4 \quad (0.50)$$

となる z が存在する。また、 $6n-1$ と同様に、

$$6y = v - 2 \quad (0.51)$$

より、 $6n+1$ のエラトステネスの篩の特殊形が完成する。

$$6n+1 \quad (0.52)$$

$$6n+1+(6n+1)(6z+4) \quad (0.53)$$

$$6n+1+(6n+1)(6z+4)+(6n+1)(6y+2) \quad (0.54)$$

したがって、ある $6n+1$ 型の素数の倍数の一般形は

$$(6n+1) \quad (0.55)$$

以下の2つは、交互に現れる。1つめは、

$$(6n+1)\{1+g(6z+4+6y+2)+6z+4\}(g\text{は自然数}) \quad (0.56)$$

$$(6n+1)\{6-1+6g(z+y+1)+6z\}(g\text{は自然数}) \quad (0.57)$$

$$(6n+1)(6c-1)(\text{但し } c = g(z+y+1)+z+1) \quad (0.58)$$

2つめは、

$$(6n + 1)\{1 + g(6z + 4 + 6y + 2) + 6z + 4 + 6y + 2\} (g \text{ は自然数}) \quad (0.59)$$

$$(6n + 1)\{1 + 6 + g(6z + 6y + 6) + 6z + 6y\} (g \text{ は自然数}) \quad (0.60)$$

$$(6n + 1)(6d + 1) (\text{但し } d = g(z + y + 1) + z + y + 1) \quad (0.61)$$

0.3 結論

● $6n-1$ のとき、

1つめは、

$$(6n - 1)(6a - 1)\{ \text{但し } a = g(z + y - 1) + z \} \quad (0.62)$$

2つめは、

$$(6n - 1)(6b + 1)\{ \text{但し } b = (g + 1)(z + y - 1) \} \quad (0.63)$$

は、素数でない。

● $6n+1$ のとき、

1つめは、

$$(6n + 1)(6c - 1)\{ \text{但し } c = g(z + y + 1) + z + 1 \} \quad (0.64)$$

2つめは、

$$(6n + 1)(6d + 1)\{ \text{但し } d = g(z + y + 1) + z + y + 1 \} \quad (0.65)$$

は、素数でない。

そして、これらの4つ式の示していることは、その積は、素数の候補同士の積であるということである。