Euler の素数生成多項式について

情報科学学科　大仲　哲平　　　指導教員：田坂　浩二

1　はじめに

Euler は、非負整数 $x = 0, 1, 2, \ldots, q-2$ において連続して素数を与える二次式 $f_q(x) = x^2 + x + q$ の研究を行った。以下、これを満たす $f_q(x)$ を Euler の素数生成多項式と呼ぶ。$f_q(q-1) = q^2$ がわかるので、x は $q-2$ までとした。また、$f_q(0) = q$ であるため、q は素数とする。これに対し、Euler は以下のことを発見した [1]。

命題 1.1　$f_q(x) = x^2 + x + q$ において、$q = 2, 3, 5, 11, 17, 41$ のとき、連続する $q-1$ 個の整数 $x = 0, 1, 2, ..., q-2$ に対して、$f_q(x)$ は素数である。

例えば､$q = 11, f_{11}(x) = x^2+x+11$ のとき､$x = 0, 1, 2, 3..., 9$ を代入したとき､$f_{11}(x)$ は $11, 13, 17, 23, 31, 41, 53, 67, 83, 101$ となり、連続して素数が現れる。

本研究では、与えられた自然数 n について、連続する n 個の整数 $x = 0, 1, 2, ..., n$ における値が素数となるようなモニック整数係数二次多項式 (これを n-素数生成多項式と呼ぶ) が存在するかを議論する。

2　先行結果

$f_q(x)$ に対し、以下のことが知られている。

定理 2.1　$m = 1 - 4q$ とおくとき、次の (1),(2) は同値である。
(1) m は平方因子を持たず、虚二次体 $\mathbb{Q}(\sqrt{m})$ の類数は 1 である。
(2) 連続する $q-1$ 個の整数 $n = 0, 1, 2, ..., q-2$ に対して、$f_q(n)$ は素数である。

(1) ⇒ (2) は 1912 年 Frobenius によって証明され、(2) ⇒ (1) は 1913 年に Rabinowitch によって証明された [1]。

類数は、”二次体の整数の素因数分解が一意的かどうかをはかる尺度”として Gauss により導入され、今日まで (代数的) 整数論における重要な研究対象となっている。類数が 1 となる虚二次体については、Baker および Stark により 1960 年代に完全なリストが与えられた。[1]

定理 2.2　(Baker(1966)・Stark(1967))
平方因子を含まない負の整数 m に対して、虚二次体 $\mathbb{Q}(\sqrt{m})$ の類数が 1 であるのは、
$m = -1, -2, -3, -7, -11, -19, -43, -67, -163$ の 9 個に限る。

定理 2.2 のリストを定理 2.1 に適用することで、Euler の素数生成多項式が命題 1.1 で与えられた 6 個しかないことがわかる。これら 6 個については、
$g_2(x) = f_2(x-1), g_3(x) = f_3(x-2), \ldots, g_{41}(x) = f_{41}(x-40)$ がそれぞれ $1, 3, 7, 19, 31, 79$-素数生成多項式であることがわかる。従って、$n \leqq 79$ については、n-素数生成多項式が必ず存在する。

しかし、$n \leqq 79$ に対する n-素数生成多項式が Euler の素数生成多項式の変形からしか得られないかは未解決である。

3　主結果

$n \geqq 1$ のとき、$f(x)$ が n-素数生成多項式ならば、$f(x)$ は 1-素数生成多項式である。まずは、1-素数生成多項式について述べる。

命題 3.1　モニック整数係数二次多項式 $x^2 + ax + b$ が 1-素数生成多項式であることの必要十分条件は、$b = s, a = r - s - 1$ をみたす素数 r, s が存在することである。

従って、n-素数生成多項式はある素数 r, s によって、
$f_{r,s} = x^2 + (r - s - 1)x + s$ と表される。

一つ目の主結果は、$n \leqq 79$ に対する n-素数生成多項式は Euler の素数生成多項式の変形からしか得られないのかという問題について、数値実験を行った結果である。

定理 3.2　素数 $r, s \leqq 3000$ に対し､$25 \leqq n \leqq 79$ とする。$f_{r,s}(x)$ が n-素数生成多項式ならば、次のいずれかと等しい。
$\{\ g_q(x+a)\ \mid\ q \in \{2, 3, 5, 11, 17, 41\},\ a \in \{0, 1, ..., q-n\}\ \}$

$n \leqq 24$ の場合に、Euler の素数生成多項式の変形ではないものが存在することが確かめられた。

また、$n \geqq 80$ に対する n-素数生成多項式が存在するかは未解決である。二つ目の主結果はこの問題について、ある条件下で非存在であることを数値実験で確かめた結果である。

定理 3.3　$f_{r,s}(x)$ が 80-素数生成多項式であるような素数 $r, s \leqq 3000$ は存在しない。

4　まとめと今後の課題

本研究では、与えられた自然数 n について、連続する n 個の整数 $x = 0, 1, 2, ..., n$ における値が素数となるようなモニック整数係数二次多項式、特に 80-素数生成多項式の存在について議論をした。主結果より、$r, s \leqq 3000$、$n \leqq 24$ では Euler の素数生成多項式に帰着されないものがあることがわかった。また、$r, s \leqq 3000$ のとき、80-素数生成多項式は存在しないことがわかった。

この数値実験では r, s に制限があったため、r, s に制限がない場合についても考える必要がある。このことから以下のことが一つ目の課題として挙げられる。

課題 1　80-素数生成多項式は存在するのか。

また、本研究ではモニック整数係数二次多項式を扱い、n-素数生成多項式の存在を議論したため、以下のことが二つ目の課題として挙げられる。

課題 2　$ax^2 + bx + c$ という形の二次式で、80-素数生成多項式は存在するのか。また、三次式以降では 80-素数生成多項式は存在するのか。

参考文献

[1] 青木昇　数学のかんどころ 15　素数と 2 次体の整数論　共立出版　2012