Korean J. Math. **30** (2022), No. 2, pp. 335–339
http://dx.doi.org/10.11568/kjm.2022.30.2.335

PRIME PRODUCING POLYNOMIALS WITH SOME DEGREES

Seungheon Lee, Geon Choi, and Jinseo Park*

Abstract. In this paper, we find the forms of polynomials which generate consecutive prime values. Then, we consider about general form of polynomials and apply on the quadratics and tertiaries.

1. Introduction

Prime-producing function has been studied by many mathematicians for a long time. Especially the quadratics, the most simple form of polynomials which can produce consecutive prime values and the exponential functions like Mersene primes and Fermat primes. These two are the most celebrated of the prime-producing exponential functions. The most celebrated of the prime-producing quadratics is $x^2 - x + 41$. It has been known as Euler's polynomial and this quadratics makes primes for all integers x with $1 \leq x \leq 40$. We can easily make a quadratics $x^2 + x + 41$ which makes primes for all integers x with $0 \leq x \leq 39$. By linear transformation, we can produce quadratics which generate consecutive prime values. However, the length of generated prime values and the discriminant are invariable. Let $R = \{r_1, \dots, r_k\}$ with $r_i \in \mathbb{Z}$ for $i = 1, \dots, k$. The set R is called admissible if there exists an integer a_q with $1 \leq a_q \leq q$ such that

$$\prod_{i=1}^{k}(a_q + r_i) \not\equiv 0 \pmod q$$

for all prime q. The famous conjecture for prime-producing function is that if R is an admissible set then there are infinitely many integers n such that $n + r$ is prime for each $r \in R$. This conjecture is called the prime k-tuples conjecture. The twin prime conjecture is the case $R = \{0, 2\}$, that is the prime k-tuples conjecture is a generalization of the twin prime conjecture. The following theorem is the most famous theorem of Prime-producing function under assumption that the prime k-tuples conjecture holds.

Theorem 1.1. [1, Theorem 2.1] *If the prime k-tuples conjecture holds, then for any positive integer B, there exists a quadratic polynomial of the form $f(x) = x^2 + x + A$, such that $f(x)$ is prime for all integer x with $0 \leq x \leq B$.*

Received February 16, 2022. Revised May 23, 2022. Accepted June 9, 2022.
2010 Mathematics Subject Classification: 11N32, 11N80.
Key words and phrases: Prime-producing function, Quadratic polynomial.
∗ Corresponding author.

In this paper, we find the another theorem under the same assumption and some conditions for the polynomial to be admissible.

2. Results

Let us find the another theorem under the prime k-tuples conjecture holds and find some conditions for the quadratic and the cubic polynomial to be admissible.

THEOREM 2.1. *Let q be a prime and $f(x)$ be a polynomial of the form*

$$f(x) = \sum_{k=0}^{2n} c_k x^k = \left(\sum_{k=0}^{n} d_k x^k \right)^2 - \beta + c_0$$

which satisfies $f(0) \equiv f(1) \pmod 2$. If the prime k-tuples conjecture holds then there exists an integer A which satisfies $f(x) + A$ is prime for all integers x with $0 \leq x \leq B$ for any positive integer B .

Proof. Let $r_j = f(j) - c_0$ for $j = 0, \ldots, B$. It is suffice to show that the set $\{r_j\}_{j=0}^{B}$ is admissible.

1. The case of $q = 2$.
   Since $f(0) \equiv f(1) \pmod 2$, we have $r_i \equiv r_j \pmod 2$ for all $0 \leq i, j \leq B$. This means there exists an integer a_2 which satisfies $\prod_{j=0}^{B} (r_j + a_2) \not\equiv 0 \pmod 2$.
2. The case of $q \geq 3$.
   By Chinese remainder theorem, we get an integer b_q which is a quadratic non-residue modulo q. Let us define $a_q = (\beta - b_q)$. If $\prod_{j=0}^{B} (r_j + a_q) \equiv 0 \pmod q$ then there exists an integer j which satisfies $r_j \equiv -a_q \pmod q$ with $0 \leq j \leq B$. This means

$$(d_n j^n + \cdots + d_1 j + d_0)^2 = \{f(j) - c_0\} + \beta = r_j + \beta \equiv -a_q + \beta \equiv b_q \pmod q,$$

   which is a contradiction.

Therefore, the set $\{r_j\}_{j=0}^{B}$ is admissible and we obtain the desired result by the prime k-tuples conjecture. □

We provide more specific conjecture of Theorem 2.1.

CONJECTURE 1. Let q be a prime and $f(x)$ be a polynomial of the form

$$f(x) = \sum_{k=0}^{2n} c_k x^k = \frac{(d_n x^n + \cdots + d_1 x + d_0)^2 - \beta}{\alpha} + c_0$$

which satisfies $f(0) \equiv f(1) \pmod 2$. If the prime k-tuples conjecture holds then there exists an integer A which satisfies $f(x) + A$ is prime for all integers x with $0 \leq x \leq B$ for any positive integer B .

To give an example of the conjecture 1,

$$\frac{\{(2x^2 + 2x + 5)^2 - 25\}}{4} + 113$$

is prime for all integers x with $0 \leq x \leq 10$.

Theorem 2.2. *Let q be an arbitrary prime and $f(x)$ be a polynomial of the form*

$$f(x) = c_k x^k + \cdots + c_1 x + c_0.$$

The set $\{f(j)\}_{j=0}^{B}$ is admissible for any positive integer B if and only if there exist two integers m, n which satisfy

$$q \mid f(m) - f(n) \quad \text{and} \quad m \not\equiv n \pmod{q}. \tag{1}$$

Proof. Let the set $\{f(j)\}_{j=0}^{B}$ be admissible. Then there exist an integer a_q which satisfies

$$\prod_{j=0}^{B} (r_j + a_q) \not\equiv 0 \pmod{q}.$$

This means $r_j \not\equiv -a_q \pmod{q}$ for all integer j with $0 \le j \le q-1$. Since $\lceil \frac{q}{q-1} \rceil = 2$, there exist two integers m, n which satisfy

$$q \mid f(m) - f(n) \quad \text{and} \quad m \not\equiv n \pmod{q}.$$

Suppose that there exist two integers m, n which satisfy two conditions (1). Since

$$f(m) \equiv f(n) \pmod{q} \quad \text{and} \quad m \not\equiv n \pmod{q},$$

then there does not exist integer j such that $f(j) \equiv r \pmod{q}$ for some r with $0 \le r \le q-1$. Let us define $a_q = q - r$. Then we find

$$\prod_{j=0}^{B} (r_j + a_q) \equiv \prod_{j=0}^{B} (r_j - r) \not\equiv 0 \pmod{q}.$$

Therefore, the set $\{f(j)\}_{j=0}^{B}$ is admissible. □

Corollary 2.3. *Let q be a prime and $f(x)$ be a polynomial*

$$f(x) = c_k x^k + \cdots + c_1 x + c_0.$$

The set $\{f(j)\}_{j=0}^{B}$ is admissible for any positive integer B if there exists an integer m which satisfies $f(m) = f(m+1) = 0$.

Proof. Since $m \not\equiv m+1 \pmod{q}$ for all prime q, $\{f(j)\}_{j=0}^{B}$ is admissible by Theorem 2.2. □

To give an example of the theorem 2.2,

- $x(x+1)(x+2) + 47$ is prime for all integers x with $0 \le x \le 10$.
- $x(x+2)(x+3) + 139$ is prime for all integers x with $0 \le x \le 15$.
- $3(x+52)(x-16)(x-17) + 41$ is prime for all integers x with $0 \le x \le 28$.

Let a^* denote a modular multiplicative inverse of an integer a. we use this notation in the rest of the paper.

Theorem 2.4. *If a quadratic polynomial of the form $f(x) = ax^2 + bx + c$ satisfies following two conditions*

$$a \equiv b \pmod{2} \quad \text{and} \quad \prod_{p \mid a} p \mid b$$

then the set $\{f(j)\}_{j=0}^{B}$ is admissible for any positive integer B.

Proof. Let us consider the case of $q = 2$. Then we easily find that $f(0) \equiv f(1) \pmod 2$ when $a \equiv b \pmod 2$. Therefore, we have $f(i) \equiv f(j) \pmod 2$ for all positive integers i, j and there exists an integer a_2 which satisfies

$$\prod_{j=1}^{B} (r_j + a_2) \not\equiv 0 \pmod 2.$$

For each prime $q \neq 2$ with $(a, q) = 1$, there exist two integers i, j which satisfy $i + j \equiv -a^* b \pmod q$ and $i \not\equiv j \pmod q$. This means

$$q \mid \{a(i+j) + b\} (i - j) = f(i) - f(j).$$

Let us consider the case $q \mid a$. Then, we have $q \mid b$ by hypothesis. This means

$$f(i) - f(j) \equiv (i - j) \{a(i+j) + b\} \equiv 0 \pmod q.$$

Therefore, we obtain the set $\{f(j)\}_{j=0}^{B}$ is admissible by Theorem 2.2. □

THEOREM 2.5. *Let q, r be primes and $f(x)$ be the polynomial of the form*

$$f(x) = ax^3 + bx^2 + cx.$$

If the set $\{f(j)\}_{j=0}^{B}$ is admissible for any positive integer B then we have

$$2 \mid a + b + c, \quad \prod_{r \mid b} r \mid c$$

and there exist integers t, s which satisfy

$$(ba^*)^2 - 3(ca^*) \equiv 3t^2 + s^2 \pmod q,$$

where q, r are odd primes with $q \nmid a,\ r \mid a$.

Proof. Let $\{f(j)\}_{j=0}^{B}$ be admissible for any positive integer B. By Theorem 2.2, there exists two integers i, j which satisfy $f(i) \equiv f(j) \pmod q$ with $0 \leq i \neq j < q$.

1. The case of $q = 2$
   There exists an integer a_2 which satisfies
   $$2 \nmid \prod_{j=0}^{B} (f(j) + a_2)$$
   and $f(0) \equiv f(1) \pmod 2$, since $\{f(j)\}_{j=0}^{B}$ is admissible. Therefore, we have
   $$2 \mid a + b + c.$$
2. The case of $q \geq 3$ with $\gcd(q, a) = 1$.
   When $q \geq 3$, $q \mid f(i) - f(j)$ means
   $$q \mid a(i+j)^2 + b(i+j) + c - aij,$$
   since $q \nmid i - j$. Let $k = i + j$ and $m = k^2 + ba^*k + ca^*$. Then we have
   $$q \mid j^2 - kj + m.$$
   This means $(2j - k)^2 \equiv k^2 - 4m \pmod q$. Let $k^2 - 4m \equiv l^2 \pmod q$. Then we get

$$(3k + 2ba^*)^2 \equiv -3l^2 - 12ca^* + 4b(a^*)^2 \pmod q. \tag{2}$$

Let us define $l = 2t, 3k + 2ba^* = 2s$. Then the equation (2) becomes

$$3t^2 + s^2 \equiv (ba^*)^2 - 3(ca^*) \pmod{q}.$$

3. The case of $q \geq 3$ with $\gcd(q, a) \neq 1$.
   If $q \mid a$ then there exist integers i, j which satisfy $q \mid b(i+j) + c$. Let us consider the case of $q \nmid b$. Then we find integers i, j which satisfy $i + j \equiv -cb^* \pmod{q}$. If $q \mid b$ then $q \mid c$. Therefore, we have

$$\prod_{r \mid b} r \mid c$$

   for all prime divisors r of a.

$\square$

References

[1] R. A. Mollin, *Prime-Producing Quadratics*, Amer. Math. Monthly **104**, (1997), 529–544.

Seungheon Lee
Institute of Science Education for the Gifted and Talented, Yonsei University, Seoul, 03722, Korea
E-mail: `snuvoice29@gmail.com`

Geon Choi
Institute of Science Education for the Gifted and Talented, Yonsei University, Seoul, 03722, Korea
E-mail: `geonchoi06@gmail.com`

Jinseo Park
Department of Mathematics Education, Catholic Kwandong University, Gangneung 25601, Korea
E-mail: `jspark@cku.ac.kr`