Chapter 5

Some irreducibility results for truncated binomial expansions

5.1 Introduction

In this chapter, for positive integers \( k \) and \( n \) with \( k \leq n - 1 \), \( P_{n,k}(x) \) denotes the polynomial \( \sum_{j=0}^{k} \binom{n}{j} x^j \), where \( \binom{n}{j} = \frac{n!}{j!(n-j)!} \). In 2007, Filaseta, Kumchev and Pasechnik considered the problem of irreducibility of \( P_{n,k}(x) \) over the field \( \mathbb{Q} \) of rational numbers. In the case \( k = 2 \), \( P_{n,2}(x) \) has discriminant \(-n^2 + 2n\) and hence is irreducible over \( \mathbb{Q} \). Another easy case is when \( k = n - 1 \). In this situation, \( P_{n,k}(x) \) is irreducible over \( \mathbb{Q} \) if and only if \( n \) is a prime number. In fact if \( n \) is a prime number, then \( x^{n-1}P_{n,n-1}(1/x) = x^{n-1} + \binom{n}{1} x^{n-2} + \cdots + \binom{n}{n-2} x + \binom{n}{n-1} \) is an Eisenstein polynomial with respect to \( n \) and if \( n \) is composite, then \( P_{n,n-1}(x) = (x + 1)^n - x^n \) is clearly reducible. In [F-K-P], Filaseta et al. proved that for any fixed integer \( k \geq 3 \), there exists an integer \( n_0 \) depending on \( k \) such that \( P_{n,k}(x) \) is irreducible over \( \mathbb{Q} \) for every \( n \geq n_0 \) (see [F-K-P, Theorem 3]). So there are indications that \( P_{n,k}(x) \) is irreducible for every \( n, k \) with \( 3 \leq k \leq n - 2 \).

In the present chapter, the irreducibility of \( P_{n,k}(x) \) is proved for those \( n, k \) for which \( 2 \leq 2k \leq n < (k + 1)^3 \). We consider the irreducibility of the polynomial

\[
P_{n,k}(x-1) = \sum_{j=0}^{k} \binom{n}{j} (x-1)^j = \sum_{j=0}^{k} \binom{n}{j} \sum_{i=0}^{j} \binom{j}{i} (-1)^{j-i} x^i = \sum_{i=0}^{k} \sum_{j=i}^{k} \binom{n}{j} \binom{j}{i} (-1)^{j-i} x^i
\]
\[ \sum_{i=0}^{k} \sum_{j=i}^{k} \binom{n}{i} \binom{n-i}{j-i} (-1)^{j-i} x^i = \sum_{i=0}^{k} \binom{n}{i} \sum_{t=0}^{k-i} \binom{n-i}{t} (-1)^t x^i = \sum_{i=0}^{k} c_i x^i, \]

where \( c_i = \binom{n}{i} \sum_{t=0}^{k-i} \binom{n-i}{t} (-1)^t \). As in [F-K-P], on using the identity
\[
\sum_{i=0}^{a} (-1)^i \binom{b}{t} = (-1)^a \binom{b-1}{a}, \quad a < b \text{ non-negative integers},
\]
a simple calculation shows that
\[
c_i = (-1)^{k-i} \frac{n(n-1) \cdots (n-i+1)(n-i+2) \cdots (n-k)}{i!(k-i)!}.
\]

In fact we shall prove the irreducibility of \( P_{n,k}(x-1) \) using Newton polygons with respect to primes strictly greater than \( k \) dividing \( \binom{n}{k} \) and some results of Erdős, Selfridge, Saradha, Shorey and Laishram regarding such primes proved in [Sa-Sh], [La-Sh]. Our method also works to prove the irreducibility of polynomials
\[
F_{n,k}(x) = \sum_{i=0}^{k} a_i c_i x^i,
\]
where \( c_i \) are as above, \( a_0, a_1, \ldots, a_k \) are non-zero integers and each \( a_i \) has all of its prime factors \( \leq k \).

Precisely stated, we prove

**Theorem 5.1.1.** Let \( k \) and \( n \) be positive integers such that \( 2k \leq n < (k+1)^3 \). Then \( P_{n,k}(x) \) is irreducible over \( \mathbb{Q} \).

Indeed we prove the following more general result from which the above theorem is quickly deduced.

**Theorem 5.1.2.** Let \( k \) and \( n \) be positive integers such that \( 8 \leq 2k \leq n < (k+1)^3 \) and \( F_{n,k}(x) \) be as in (5.2). Then \( F_{n,k}(x) \) is irreducible over \( \mathbb{Q} \) except possibly when \( (n,k) \) belongs to the set \( \{(8,4),(10,5),(12,6),(16,8)\} \).

It may be pointed out that the polynomial \( F_{10,5}(x) \) with \( c_i \) as defined in (5.1) given by
\[
F_{10,5}(x) = 2000 \cdot c_5 x^5 - 375 \cdot c_4 x^4 - 9 \cdot c_3 x^3 + 10 \cdot c_2 x^2 - 27 \cdot c_1 x + 25 \cdot c_0
\]
has $7x^2 + 7x + 1$ as a factor which shows that Theorem 5.1.2 indeed has exceptions.

In the course of the proof of Theorem 5.1.2, we prove the following result which is of independent interest as well.

**Theorem 5.1.3** Let $k, n$ be integers such that $n \geq k + 2 \geq 4$. Suppose there exists a prime $p > k$, $p$ divides a number $n - l, 1 \leq l \leq k - 1$, with exact power $e \geq 1$ such that $gcd(e, l) \leq 2$ and $gcd(e, k - l) \leq 2$. If $l_1 < k/2$ is a positive integer such that $l \not\in \{l_1, 2l_1, k - l_1, k - 2l_1\}$, then $F_{n,k}(x)$ cannot have a factor of degree $l_1$ over $\mathbb{Q}$.

### 5.2 Notations and Preliminary Results

Let $p$ be a prime number. For any non-zero integer $a$, $v_p(a)$ will denote the $p$-adic valuation of $a$, i.e., the highest power of $p$ dividing $a$ and $v_p(0)$ will be denoted by $\infty$. Let $f(x) = \sum_{j=0}^{n} a_j x^j$ be a polynomial over $\mathbb{Q}$ with $a_0 a_n \neq 0$. Let $P_i$ stand for the point in the plane having coordinates $(i, v_p(a_{n-i}))$ with $a_{n-i} \neq 0$, $0 \leq i \leq n$. Let $\mu_{ij}$ denote the slope of the line joining the points $P_i$ and $P_j$ when $a_{n-j}a_{n-j} \neq 0$. Let $i_1$ be the largest index $0 < i_1 < n$ such that $\mu_{0i_1} = \min\{\mu_{0j} | 0 < j \leq n, a_{n-j} \neq 0\}$. If $i_1 < n$, let $i_2$ be the largest index such that $i_1 < i_2 \leq n$ and $\mu_{i_1i_2} = \min\{\mu_{ij} | i_1 < j \leq n, a_{n-j} \neq 0\}$ and so on. The Newton polygon of $f(x)$ with respect to $p$ is the polygonal path having segments $P_0P_{i_1}, P_{i_1}P_{i_2}, \ldots, P_{n-1}P_{i_k}$ with $i_k = n$. These segments are called the edges of the Newton polygon and their slopes form a strictly increasing sequence.

We state below a well-known result to be used in the sequel (see [Rib2, 5.1.F]).

**Theorem 5.2.A.** Let $(x_0, y_0), (x_1, y_1), \ldots, (x_r, y_r)$ denote the successive vertices of the Newton polygon of a polynomial $g(x)$ with respect to a prime $p$. Let $\tilde{v}_p$ denote the unique extension of $v_p$ to the algebraic closure of the field $\mathbb{Q}_p$ of $p$-adic numbers. Then $g(x)$ factors over $\mathbb{Q}_p$ as $g_1(x)g_2(x) \cdots g_r(x)$ where the degree of $g_i(x)$ is...
\[ x_i - x_{i-1}, \, i = 1, 2, \ldots, r \] and all the roots of \(g_i(x)\) in the algebraic closure of \(\mathbb{Q}_p\) have \(v_p\) valuation \(\frac{b_i - a_i}{x_i - x_{i-1}}\). In particular all the roots of an irreducible factor of \(g(x)\) over \(\mathbb{Q}_p\) will have the same \(v_p\) valuation.

**Notations.** For an integer \(\nu > 1\), let \(P(\nu)\) denote the greatest prime divisor of \(\nu\) and let \(\pi(\nu)\) denote the number of primes not exceeding \(\nu\). For a real number \(\rho\), \([\rho]\) stands for the greatest integer not exceeding \(\rho\). As in [La-Sh], \(\delta(k)\) will denote the integer defined for \(k \geq 3\) by
\[
\delta(k) = \begin{cases} 
2, & \text{if } 3 \leq k \leq 6; \\
1, & \text{if } 7 \leq k \leq 16; \\
0, & \text{otherwise}.
\end{cases}
\]

For numbers \(n, k\) and \(h\), \([n, k, h]\) will stand for the set of all pairs \((n, k), (n+1, k), \ldots, (n+h-1, k)\). In particular \([n, k, 1] = \{(n, k)\}\).

As in [La-Sh], we shall denote by \(S\) the union of the sets
\[
[6, 3, 1], [8, 3, 3], [18, 3, 1], [9, 4, 1], [10, 5, 4], [16, 5, 1], [18, 5, 3], [27, 5, 2], [12, 6, 2], [20, 6, 1], [14, 7, 3], [18, 7, 1], [20, 7, 2], [30, 7, 1], [16, 8, 1], [21, 8, 1], [26, 13, 3], [30, 13, 1], [32, 13, 2], [36, 13, 1], [28, 14, 1], [33, 14, 1], [36, 17, 1]
\]
and by \(T\) the union of the sets
\[
[38, 19, 3], [42, 19, 1], [40, 20, 1], [94, 47, 3], [100, 47, 1], [96, 48, 1], [144, 71, 2], [145, 72, 1], [146, 73, 3], [156, 73, 1], [148, 74, 1], [162, 79, 1], [166, 83, 1], [172, 83, 1], [190, 83, 1], [192, 83, 1], [178, 89, 1], [190, 89, 1], [192, 89, 1], [210, 103, 2], [212, 103, 2], [216, 103, 2], [213, 104, 1], [217, 104, 1], [214, 107, 12], [216, 108, 10], [218, 109, 9], [220, 110, 7], [222, 111, 5], [224, 112, 3], [226, 113, 7], [250, 113, 1], [252, 113, 2], [228, 114, 5], [253, 114, 1], [230, 115, 3], [232, 116, 1], [346, 173, 1], [378, 181, 1], [380, 181, 2], [381, 182, 1], [392, 193, 2], [393, 194, 1], [396, 197, 1], [398, 199, 3], [400, 200, 1], [552, 271, 5], [553, 272, 1], [555, 272, 2], [556, 273, 1], [554, 277, 3], [558, 277, 5], [556, 278, 1], [559, 278, 4], [560, 279, 3], [561, 280, 1], [562, 281, 7], [564, 282, 5], [566, 283, 5], [576, 283, 1], [568, 284, 3], [570, 285, 1], [586, 293, 1].
\]

With the above notations, the following theorem due to Laishram and Shorey
[La-Sh, Theorem 3] holds.

**Theorem 5.2.B.** Let \( n \geq 2k \geq 6 \) and \( f_1 < f_2 < \cdots < f_\mu \) be integers in \([0,k)\). Assume that the greatest prime factor of \((n - f_1)\cdots(n - f_\mu) \leq k\). Then \( \mu \leq k - \left[ \frac{3}{4} \pi(k) \right] + 1 - \delta(k) \) unless \((n,k) \in S \cup T\).

The corollary stated below is an immediate consequence of Theorem 5.2.B in view of the fact that \( k - \mu \geq \left[ \frac{3}{4} \pi(k) \right] - 1 \geq 5 \) for \( k \geq 19\).

**Corollary 5.2.C.** Let \( n \) and \( k \) be positive integers with \( n \geq 2k \geq 38 \). Then there are at least five distinct terms of the product \( n(n - 1)\cdots(n - k + 1) \) each divisible by a prime exceeding \( k \) except when \((n,k) \in T\).

The following two theorems are used in the proof of Proposition 5.2.1 (see [Sa-Sh, Theorem 2, Theorem A]).

**Theorem 5.2.D.** For \( n > k^2 \geq 5^2 \) the equation \( n(n + 1)\cdots(n + i - 1)(n + i + 1)\cdots(n + k - 1) = by^2 \) has no solution in positive integers \( n, k, b, y \) with \( P(b) \leq k \) and \( 0 < i < k - 1 \).

**Theorem 5.2.E.** For \( n > k^2 \geq 4^2 \) the equation \( n(n + 1)\cdots(n + k - 1) = by^2 \) has no solution in positive integers \( n, k, b, y \) with \( P(b) \leq k \).

We now prove some results to be used in the proof of Theorem 5.1.3.

**Proposition 5.2.1.** Let \( k \geq 6 \) and \( n > k^2 \). Then there exist two distinct terms \( n + r \) and \( n + s \) of the product \( n(n + 1)\cdots(n + k - 1) \) which are divisible by primes \( > k \) exactly to an odd power.

**Proof.** Suppose the proposition is false for some \( n \) and \( k \) with \( k \geq 6 \) and \( n > k^2 \). Let \( \Delta(n,k) = n(n + 1)\cdots(n + k - 1) \). Thus either \( v_p(\Delta(n,k)) \) is even for all primes \( p > k \) or there is exactly one term \( n + i \) and a prime \( p > k \) such that \( v_p(\Delta(n,k)) \) is odd. The first possibility is excluded since for any positive integer \( b \) with \( P(b) \leq k \), the equation

\[
n(n + 1)\cdots(n + k - 1) = by^2
\]
has no solution in positive integers \( n, k, y \) when \( n > k^2 \geq 4^2 \) by Theorem 5.2.E. We now consider the case when there is exactly a term \( n+i \) and a prime \( p > k \) such that \( \nu_p(\Delta(n,k)) \) is odd. Suppose first that \( 0 < i < k - 1 \). Removing the term \( n+i \) from \( \Delta(n,k) \), we see that \( n(n+1) \cdots (n+i-1)(n+i+1) \cdots (n+k-1) = b_1y_1^2 \) where \( P(b_1) \leq k \) which is impossible by virtue of Theorem 5.2.D.

It remains to consider the case when \( i = 0 \) or \( k - 1 \). Let \( \Delta' \) denote the product \( (n+1) \cdots (n+k-1) \) or \( n(n+1) \cdots (n+k-2) \) according as \( i = 0 \) or \( k - 1 \). Then \( \Delta' \) is a product of \( k - 1 \) consecutive integers such that

\[
\Delta' = b_2y_2^2
\]

with \( P(b_2) \leq k \). This is impossible when \( P(b_2) \leq k - 1 \) by Theorem 5.2.E. It only remains to deal with the situation when \( P(b_2) = k \). Then \( k \) will be a prime dividing only one term of the product \( \Delta' \), say \( k \) divides \( n+j, j \neq i \). We remove the term \( n+j \) of the product \( \Delta' \) and it is clear from (5.3) that

\[
\frac{\Delta'}{n+j} = b_3y_3^2, \quad P(b_3) \leq k - 2.
\]

It is immediate from (5.4) and Theorem 5.2.D that \( n+j \) is the first or last term of the product \( \Delta' \) as \( k - 1 \geq 5 \). Thus we see that \( \frac{\Delta'}{n+j} \) is the product of \( k - 2 \) consecutive integers. This is impossible by Theorem 5.2.E.

**Proposition 5.2.2.** Let \( n, k \) be positive integers with \( n \geq k + 2 \geq 4 \) and \( F_{n,k}(x) \) be given by (5.2). Suppose there exists a prime \( p > k \) such that \( e \geq 1 \) is the exact power of \( p \) dividing \( n-l \) for some \( l, 1 \leq l \leq k - 1 \). Let \( d = \gcd(e,l) \) and \( d' = \gcd(e,k-l) \).

Then the following hold.

(i) The edges of the Newton polygon of \( F_{n,k}(x) \) with respect to \( p \) have slopes \( \frac{e}{k-l}, \frac{e}{l} \).

(ii) Each irreducible factor of \( F_{n,k}(x) \) over \( \mathbb{Q}_p \) has degree a multiple of \( \frac{l}{d} \) or of \( \frac{k-l}{d'} \) and there exists at least one irreducible factor of each of these two types.

(iii) If \( d = d' = 1 \), then \( F_{n,k}(x)/a_kc_k \) factors over \( \mathbb{Q}_p \) as a product of two distinct monic irreducible polynomials of degrees \( l \) and \( k - l \).
Proof. We consider the Newton polygon of $F_{n,k}(x)$ with respect to the prime $p$. In view of (5.1), the vertices of the Newton polygon are $(0,e), (k-l,0), (k,e)$. Thus the Newton polygon has two edges, one from $(0,e)$ to $(k-l,0)$ and other from $(k-l,0)$ to $(k,e)$ with respective slopes $\frac{e}{k-l}$ and $\frac{e}{l}$ proving (i).

Using Theorem 5.2.A, it follows that $F_{n,k}(x)$ factors over $\mathbb{Q}_p$ as $g(x)h(x)$ where degree of $g(x) = k-l$ and degree of $h(x) = l$. It will be shown that each irreducible factor of $g(x)$ over $\mathbb{Q}_p$ has degree a multiple of $\frac{1}{d}$ or $\frac{k-l}{d}$. Let $g_1(x)$ be an irreducible factor of $g(x)$ over $\mathbb{Q}_p$ and $\alpha$ be a root of $g_1(x)$ in the algebraic closure of $\mathbb{Q}_p$. Let $\nu_p$ be as in Theorem 5.2.A and $\nu'$ denote the valuation of $\mathbb{Q}_p(\alpha)$ obtained by restricting $\nu_p$. Then by Theorem 5.2.A,

$$\nu'(\alpha) = \frac{-e}{k-l} = \frac{-e/d}{(k-l)/d}.$$ 

So $\frac{k-l}{d}$ divides the index of ramification of $\nu'/\nu_p$ which divides $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = \deg g_1(x)$. Arguing similarly we see that any irreducible factor $h_1(x)$ of $h(x)$ over $\mathbb{Q}_p$ has degree a multiple of $l/d$. Hence assertion (ii) follows. Assertion (iii) is an immediate consequence of (ii).

The last assertion quickly yields the following result.

**Corollary 5.2.3.** If for a pair $(n,k)$, $n \geq k+2$, there exist terms $n-l', n-l'', 1 \leq l' < l'' < k$, divisible respectively by primes $p', p''$ exceeding $k$ exactly to the first power such that $l' + l'' \neq k$, then $F_{n,k}(x)$ is irreducible over $\mathbb{Q}$.

The following proposition is already known (cf. [F-K-P, Lemma 1]). For the sake of completeness, it is proved here.

**Proposition 5.2.4.** Let $n,k$ and $F_{n,k}(x)$ be as in Proposition 5.2.2. Let $p$ be a prime $> k$ and $e > 0$ be such that $\nu_p(n) = e$. Then every irreducible factor of $F_{n,k}(x)$ over $\mathbb{Q}_p$ has degree a multiple of $\frac{k}{D}$, where $D = \gcd(e,k)$.

Proof. The vertices of the Newton polygon of $F_{n,k}(x)$ with respect to $p$ are $(0,e), (k,0)$. Thus the Newton polygon has only one edge whose slope is $-e/k$. So arguing as in Proposition 5.2.2, any irreducible factor of $F_{n,k}(x)$ must have degree a multiple of $k/D$. 

49
5.3 Proof of Theorem 5.1.3

Using Proposition 5.2.2 (with \(d, d'\) atmost 2), it follows that each irreducible factor of \(F_{n,k}(x)\) over \(\mathbb{Q}_p\) has degree belonging to \(\left\{ \frac{l}{2}, l, \frac{k-l}{2}, k-l \right\}\) and the factorisation of \(F_{n,k}(x)\) into irreducible factors over \(\mathbb{Q}_p\) is given by \(F(x)G(x)\) or \(F_1(x)F_2(x)G(x)\) or \(F(x)G_1(x)G_2(x)\) or \(F_1(x)F_2(x)G_1(x)G_2(x)\) where \(F(x), G(x)\) are of degree \(l, k-l\) respectively and \(F_i(x), G_i(x)\) have degrees \(l/2, (k-l)/2\) respectively for \(1 \leq i \leq 2\). Consequently any irreducible factor of \(F_{n,k}(x)\) over \(\mathbb{Q}\) must have degrees in the set

\[
\left\{ \frac{l}{2}, l, \frac{k-l}{2}, k-l, \frac{2k-l}{2}, \frac{k+l}{2}, k \right\}.
\]

Given that \(l < k\), the elements of this set that can be less than \(k/2\) are \(l/2, l, (k-l)/2\) and \(k-l\). The conditions in Theorem 5.1.3 imply that \(l_1\) is not among \(l/2, l, (k-l)/2\) and \(k-l\), so the theorem follows.

5.4 Proof of Theorems 5.1.2 and 5.1.1

With \(S\) and \(T\) as in Theorem 5.2.B, we first prove

Lemma 5.4.1. For \((n, k) \in S \cup T, k \geq 4, F_{n,k}(x)\) is irreducible over \(\mathbb{Q}\) except possibly when \((n, k)\) belongs to the subset \(S'\) of \(S\) given by \(S' = \{(10,5), (12,6), (16,8)\}\).

Proof. Let \(S''\) denote the subset of \(S\) given by

\[
S'' = \{(9,4), (12,5), (16,5), (18,5), (27,5)\}.
\]

Observe that if \(n\) is divisible by a prime \(p > k\) with \(v_p(n) = 1,\) then \(x^kF_{n,k}(1/x)\) is an Eisenstein polynomial with respect to \(p\) and so \(F_{n,k}(x)\) is irreducible over \(\mathbb{Q}\). Further if two distinct terms \(n - l_1, n - l_2\) of the product \(n(n-1) \cdots (n-k+1)\) are divisible by primes \(p_1\) and \(p_2\) exceeding \(k\) such that \(v_{p_1}(n - l_1) = 1\) and \(l_1 + l_2 \neq k\), then in view of the above observation and Corollary 5.2.3, \(F_{n,k}(x)\) is irreducible over \(\mathbb{Q}\). For each \((n, k)\) belonging to \(T \cup (S \setminus S' \cup S'')\) with \(n\) not divisible by any prime \(> k\) up to the first power, Table 1 at the end of this section indicates two primes \(p_1\) and \(p_2\) satisfying the above property. It can be easily seen that for \((n, k) \in S''\), \(F_{n,k}(x)\) is an Eisenstein polynomial with respect to the prime 5, \(F_{12,5}(x)\) is Eisenstein.
with respect to 7, $F_{18,5}(x)$, $F_{27,5}(x)$ are Eisenstein with respect to 11 and $F_{18,5}(x)$ is Eisenstein with respect to 13. Hence the lemma is proved.

**Lemma 5.4.2.** For $8 \leq n < 5^3$, the polynomial $F_{n,A}(x)$ is irreducible over $\mathbb{Q}$ except possibly when $n$ belongs to the set $U = \{8, 50, 98, 100\}$.

**Proof.** As pointed out in the proof of Lemma 5.4.1, we need to verify the irreducibility of $F_{n,A}(x)$ when $n$ is not divisible by any prime more than 4 exactly with the first power. For such $n$ not exceeding 124 and $n$ not belonging to the set $\{8, 9, 18, 27, 50, 98, 100\}$, Table 2 at the end of this section indicates two terms $n - l', n - l''$, $1 \leq l', l'' \leq 3$, $l' + l'' \neq 4$ such that $n - l', n - l''$ are divisible by primes $p', p''$ (respectively) up to the first power only. So the lemma is proved in view of Corollary 5.2.3 and the fact that $F_{9,4}$, $F_{18,4}$ and $F_{27,4}$ are Eisenstein polynomials with respect to primes 5, 7 and 23 respectively.

**Proof of Theorem 5.1.2.** We divide the proof into two cases.

**Case I.** $8 \leq 2k \leq n < (k + 1)^2$. Note that the theorem is already proved in the present case for $k = 4$ by virtue of Lemma 5.4.2, so it may be assumed that $k \geq 5$ here. Applying Theorem 5.2.B, we see that there exist at least three terms $n - l_i$, $i \in \{1, 2, 3\}$ which are divisible by primes exceeding $k$ exactly up to the first power unless $(n, k) \in S \cup T$. Using Proposition 5.2.2 (iii), $F_{n,k}(x)/\alpha_k c_k$ factors over $\mathbb{Q}_{\alpha_k}$ as a product of two distinct monic irreducible polynomials of degree $l_i$ and $k - l_i$ for $1 \leq i \leq 3$. If $F_{n,k}(x)$ were reducible over $\mathbb{Q}$, then $F_{n,k}(x)$ will have a factorization of the type $F_{n,k}(x) = \alpha_k c_k G_i(x) H_i(x)$ where $G_i(x), H_i(x)$ are monic irreducible polynomials belonging to $\mathbb{Q}[x]$ with degrees $k - l_i, l_i$ respectively. This is impossible as $l_1, l_2$ and $l_3$ are distinct. So the theorem is proved in the present case when $(n, k)$ does not belong to $S \cup T$. When $(n, k) \in (S \setminus S') \cup T$ with $k \geq 4$, the irreducibility of $F_{n,k}(x)$ follows from Lemma 5.4.1.

**Case II.** $k \geq 4$, $(k + 1)^2 \leq n < (k + 1)^3$. In this case, we first show that $F_{n,k}(x)$ cannot factor over $\mathbb{Q}$ as a product of two irreducible polynomials of degree $k/2$ each. For this it is enough to show that there exists $l' \neq k/2$, $0 \leq l' \leq k - 1$ such that $n - l'$
is divisible by a prime \( p' > k \) exactly with the first power. If \( l' = 0 \), then as pointed out in the opening lines of the proof of Lemma 5.4.1, \( F_{n,k}(x) \) is irreducible over \( \mathbb{Q} \).

If \( l' > 1 \) then by Proposition 5.2.2 (iii), \( F_{n,k}(x) \) has two irreducible factors of degree \( l' \) and \( k - l' \) over \( \mathbb{Q}_{p'} \). This leads to a contradiction as \( l' \neq k/2 \) thereby proving the irreducibility of \( F_{n,k}(x) \) over \( \mathbb{Q} \). The existence of a term \( n - l' \neq n - \frac{k}{2} \), \( 0 < l' < k - 1 \), which is divisible by some prime \( p' > k \) with \( v_{p'}(n - l') = 1 \) is guaranteed for \( k \geq 6 \) by Proposition 5.2.1 as \( (k + 1)^2 \leq n < (k + 1)^3 \) in the present situation. This proves the assertion stated in the opening lines of Case II.

It only remains to be shown that \( F_{n,k}(x) \) cannot have a factor of degree less than \( k/2 \) over \( \mathbb{Q} \). Suppose to the contrary that it has a factor of degree \( l_1 < k/2 \) over \( \mathbb{Q} \).

We make some claims.

**Claim 1:** \( P(n) \leq k \).

Suppose not. Let \( p \) be a prime \( > k \) dividing \( n \) with exact power \( e \geq 1 \). Then \( e \leq 2 \) since \( n < (k + 1)^3 \). So by Proposition 5.2.4, every irreducible factor of \( F_{n,k}(x) \) over \( \mathbb{Q}_p \) has degree a multiple of \( k \) or \( \frac{k}{2} \) according as \( e = 1 \) or 2 respectively. This is not possible in view of our supposition.

**Claim 2:** There are at most four distinct terms in the product \( n(n - 1) \cdots (n - k + 1) \) each of which is divisible by some prime \( > k \).

Assume the contrary. Then there is a term \( n - l \) with \( 0 \leq l < k \) and a prime \( p > k \) with \( p \) dividing \( (n - l) \) such that \( l \notin \{ l_1, 2l_1, k - l_1, k - 2l_1 \} \) where \( l_1 \) is as in the paragraph preceding Claim 1. Note that \( l > 0 \) in view of Claim 1. Further \( e = v_p(n - l) \leq 2 \) implying that \( F_{n,k}(x) \) cannot have a factor of degree \( l_1 \) over \( \mathbb{Q} \) by Theorem 5.1.3, which contradicts our supposition made just before Claim 1.

**Claim 3:** There are at most two distinct terms in the product \( n(n - 1) \cdots (n - k + 1) \) which are divisible by a prime \( > \sqrt{n} \).

Suppose not. Let \( 1 \leq l'_1 < l'_2 < l'_3 \) be such that there exist primes \( p_i > \sqrt{n} \) with \( p_i \) dividing \( n - l'_i \). Note that \( v_{p_i}(n - l'_i) = 1 \) for \( 1 \leq i \leq 3 \). Then \( e_i = 1 \) for each \( i \in \{1, 2, 3\} \). Since \( (k + 1)^2 \leq n \), in view of Proposition 5.2.2 (iii), it follows that \( F_{n,k}(x) \) factors over \( \mathbb{Q}_{p_i} \) as a product of two non-associate irreducible polynomials.
of degree $l_i'$ and $k - l_i'$ for $1 \leq i \leq 3$. Arguing as in Case I, we get a contradiction as $l_1', l_2'$ and $l_3'$ are distinct.

From Claim 2, Corollary 5.2.C and Lemma 5.4.1, it follows that $k \leq 18$. Note that for $k = 4$, in view of Lemma 5.4.2, we have only to consider $n = 50, 98, 100$ as $5^2 \leq n < 125$. For each of these values of $n$, $F_{n,k}(x)$ must be irreducible over $\mathbb{Q}$ by virtue of Claim 1, as $P(n)$ is more than 4. For $k \geq 5$, by virtue of Claim 1, we may first restrict to those $n$ for which $P(n) \leq k$. Further by Claims 2 and 3, those $n$ can be excluded for which $n(n - 1) \cdots (n - k + 1)$ has either five terms divisible by a prime $> k$ or three terms divisible by a prime $> \sqrt{n}$. We use Sage mathematics software for the above computations. Then we are left with the following pairs $(n, k)$ given by

$$(50, 5), (64, 5), (100, 5), (128, 5), (200, 5), (50, 6).$$

All these pairs satisfy the hypothesis of Corollary 5.2.3 as is clear from Table 3. This completes the proof of the theorem.

**Proof of Theorem 5.1.1**

In view of Theorem 5.1.2., we need to prove the irreducibility of $P_{n,k}(x)$ only when $1 \leq k \leq 3$ with $2k \leq n < (k + 1)^3$ or $(n, k)$ belongs to $\{(8, 4), (10, 5), (12, 6), (16, 8)\}$. Using Maple, we have verified the irreducibility of $P_{n,k}(x)$ for these values of $(n, k)$. 

53
<table>
<thead>
<tr>
<th>$(n, k)$</th>
<th>$E[n, k, h]$</th>
<th>Primes $(n, k)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>20, 5, 1</td>
<td>17, 19</td>
<td>162, 79, 1</td>
</tr>
<tr>
<td>20, 6, 1</td>
<td>17, 19</td>
<td>166, 83, 1</td>
</tr>
<tr>
<td>14, 7, 3</td>
<td>11, 13</td>
<td>172, 83, 1</td>
</tr>
<tr>
<td>18, 7, 1</td>
<td>13, 17</td>
<td>190, 83, 1</td>
</tr>
<tr>
<td>20, 7, 1</td>
<td>17, 19</td>
<td>192, 83, 1</td>
</tr>
<tr>
<td>21, 7, 1</td>
<td>17, 19</td>
<td>178, 89, 1</td>
</tr>
<tr>
<td>30, 7, 1</td>
<td>13, 29</td>
<td>190, 89, 1</td>
</tr>
<tr>
<td>21, 8, 1</td>
<td>17, 19</td>
<td>192, 89, 1</td>
</tr>
<tr>
<td>26, 13, 3</td>
<td>19, 23</td>
<td>210, 103, 1</td>
</tr>
<tr>
<td>30, 13, 1</td>
<td>19, 23</td>
<td>212, 103, 2</td>
</tr>
<tr>
<td>32, 13, 2</td>
<td>29, 31</td>
<td>216, 103, 2</td>
</tr>
<tr>
<td>36, 13, 1</td>
<td>29, 31</td>
<td>213, 104, 1</td>
</tr>
<tr>
<td>28, 14, 1</td>
<td>17, 19</td>
<td>217, 104, 1</td>
</tr>
<tr>
<td>33, 14, 1</td>
<td>29, 31</td>
<td>214, 107, 12</td>
</tr>
<tr>
<td>36, 17, 1</td>
<td>29, 31</td>
<td>216, 108, 10</td>
</tr>
<tr>
<td>38, 19, 3</td>
<td>23, 29</td>
<td>218, 109, 9</td>
</tr>
<tr>
<td>42, 19, 1</td>
<td>37, 41</td>
<td>220, 110, 7</td>
</tr>
<tr>
<td>40, 20, 1</td>
<td>31, 37</td>
<td>222, 111, 5</td>
</tr>
<tr>
<td>94, 47, 3</td>
<td>89, 83</td>
<td>224, 112, 3</td>
</tr>
<tr>
<td>100, 47, 1</td>
<td>83, 89</td>
<td>226, 113, 7</td>
</tr>
<tr>
<td>96, 48, 1</td>
<td>79, 83</td>
<td>250, 113, 1</td>
</tr>
<tr>
<td>114, 71, 2</td>
<td>101, 103</td>
<td>252, 113, 2</td>
</tr>
<tr>
<td>145, 72, 1</td>
<td>101, 103</td>
<td>228, 114, 5</td>
</tr>
<tr>
<td>146, 73, 3</td>
<td>101, 103</td>
<td>253, 114, 1</td>
</tr>
<tr>
<td>156, 73, 1</td>
<td>109, 113</td>
<td>230, 115, 3</td>
</tr>
<tr>
<td>148, 74, 1</td>
<td>107, 113</td>
<td>232, 116, 1</td>
</tr>
</tbody>
</table>
Table 2.

<table>
<thead>
<tr>
<th>n</th>
<th>n − l', n − l'', p', p''</th>
<th>n</th>
<th>n − l', n − l'', p', p''</th>
<th>n</th>
<th>n − l', n − l'', p', p''</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>10, 11, 5, 11</td>
<td>48</td>
<td>46, 47, 23, 47</td>
<td>81</td>
<td>79, 80, 79, 5</td>
</tr>
<tr>
<td>16</td>
<td>14, 15, 7, 5</td>
<td>49</td>
<td>46, 47, 23, 47</td>
<td>96</td>
<td>94, 95, 47, 19</td>
</tr>
<tr>
<td>25</td>
<td>22, 23, 11, 23</td>
<td>64</td>
<td>62, 63, 31, 7</td>
<td>121</td>
<td>119, 120, 17, 5</td>
</tr>
<tr>
<td>32</td>
<td>30, 31, 5, 31</td>
<td>72</td>
<td>70, 71, 5, 71</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>34, 35, 17, 5</td>
<td>75</td>
<td>73, 74, 73, 37</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3.

<table>
<thead>
<tr>
<th>(n, k)</th>
<th>n − l', n − l''</th>
<th>(n, k)</th>
<th>n − l', n − l''</th>
<th>(n, k)</th>
<th>n − l', n − l''</th>
</tr>
</thead>
<tbody>
<tr>
<td>(50, 5)</td>
<td>46, 47</td>
<td>(100, 5)</td>
<td>97, 99</td>
<td>(200, 5)</td>
<td>197, 199</td>
</tr>
<tr>
<td>(64, 5)</td>
<td>61, 63</td>
<td>(128, 5)</td>
<td>126, 127</td>
<td>(50, 6)</td>
<td>46, 47</td>
</tr>
</tbody>
</table>