Chapter 1

Preliminaries

In this chapter, we present all the definitions and basic concepts needed in our work. To make the thesis self-contained, we state all the results that are relevant in this thesis.

1.1 Basic concepts of graph theory

By a directed graph or digraph we mean a finite non-empty set of objects called vertices together with a set of ordered pairs of vertices called directed edges or simply edges. We say that there is an edge from a vertex $a$ to a vertex $b$ if $a$ is adjacent to $b$. The outdegree of a vertex $v$ is the number of vertices that are adjacent from $v$. The indegree of a vertex $v$ is the number of vertices that are adjacent to $v$. Two digraphs are said to be isomorphic if there is a bijection between the respective set of vertices that also preserves the direction of the edges. A cycle in a digraph is a sequence of adjacent vertices, written as $x \rightarrow x_1 \rightarrow \ldots \rightarrow x_n \rightarrow x$. The length of a cycle is the number of vertices in the cycle, and a cycle of length $t$ is called a $t$-cycle. A digraph $H$ is a subdigraph of $G$ if all vertices and edges of $H$ are vertices and edges from $G$. A digraph is said to be connected if there is a directed edge between every pair of vertices in it. A component of a digraph $G$ is a maximal connected subdigraph of $G$. A directed tree or simply a tree of a digraph $G$ is a subdigraph of $G$ which contains
Section 1.2 Carmichael Function

exactly one cycle vertex and all the non-cycle vertices are oriented towards the cycle vertex. A direct product of two digraphs $G$ and $H$, denoted by $G \times H$, is a digraph with vertex set $V(G) \times V(H)$ for which there is a directed edge from $(x, y)$ to $(u, v)$ in $G \times H$ if and only if there is a directed edge from $x$ to $u$ and $y$ to $v$ in $G$ and $H$, respectively. The direct product of digraphs is commutative and associative (see [16]).

1.2 Carmichael function

One of the most important and fundamental tools that will be used in this thesis is a number-theoretic function called the Carmichael lambda function. In this section we define this function and state its basic properties.

**Definition 1.2.1.** The Carmichael lambda function of a positive integer $n$, denoted by $\lambda(n)$, is defined as the smallest positive integer $m$ such that $a^m \equiv 1 \pmod{n}$ for every integer $a$ relatively prime to $n$.

This function is named after the mathematician R.D. Carmichael. In his paper [8], he defined this function by means of the Euler’s totient $\phi$-function, and we state it in the following theorem:

**Theorem 1.2.2** (Carmichael, [8]). Let $n$ be a positive integer. Then

$$\lambda(2^k) = \phi(2^k) \quad \text{for} \ k = 0, 1, 2, \quad \lambda(2^k) = \frac{1}{2}\phi(2^k) \quad \text{for} \ k \geq 3,$$

$$\lambda(p^k) = \phi(p^k) \quad \text{for any odd prime} \ p \text{ and} \ k \geq 1,$$

$$\lambda\left(\prod_{i=1}^{r} p_i^{e_i}\right) = \text{lcm}\{\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_r^{e_r})\},$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $e_i \geq 1$ for all $i = 1, 2, \ldots r$.

**Theorem 1.2.3** (Carmichael, [8]). Let $a$ and $n$ be positive integers. Then $a^{\lambda(n)} \equiv 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$. Moreover, there exists an integer $g$ such that $\text{ord}_a(g) = \lambda(n)$.
Algebraically, the Carmichael lambda function is the exponent of the multiplicative group of integers modulo $n$.

**Remark 1.2.4.** Let $a$, $b$ and $c$ be positive integers.

(a) If $a | b$ then $\lambda(a) | \lambda(b)$.

(b) $gcd(\lambda(ab), c) = lcm[gcd(a, c), gcd(b, c)]$.

### 1.3 The digraphs $G(n, k)$

**Definition 1.3.1.** Let $S$ be a non-empty set, and $f : S \rightarrow S$ be a map. An iteration digraph of $f$ is a directed graph whose vertex set is $S$ and for which there is a directed edge from $x$ to $f(x)$ for all $x \in S$.

We start by fixing some notations that will be used throughout the first three chapters. Unless specified otherwise, let $n > 1$ denote an integer expressed as

$$n = \prod_{i=1}^{r} p_i^{e_i}$$  \hspace{1cm} (1.3.1)

where the $p_i$'s are distinct primes and $e_i \geq 1$, for all $i$ such that $1 \leq i \leq r$. Let $p$ always denote a prime, and $e \geq 1$, $k \geq 2$ are integers.

Consider a map $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$. For each pair of integers $n$ and $k$, a digraph $G(n, k)$ is defined as an iteration digraph of $f$ where $f$ is defined as

$$f(x) = x^k \quad \text{for all } x \in \mathbb{Z}_n.$$

This type of iteration digraph will be the main topic of study in this thesis. Equivalently, a digraph $G(n, k)$ can also be defined as one with vertex set \{0, 1, \ldots, n - 1\} and for which there is a directed edge from $a$ to $b$ if $a^k \equiv b \pmod{n}$. These digraphs are also referred to as power digraphs modulo $n$.

Now we define two particular subdigraphs of $G(n, k)$, denoted by $G_1(n, k)$ and $G_2(n, k)$, where $G_1(n, k)$ is the subdigraph induced on the set of vertices
that are relatively prime to \( n \), and \( G_2(n, k) \) is the subdigraph induced on the set of vertices not relatively prime to \( n \). It is clear that there is no edge between \( G_1(n, k) \) and \( G_2(n, k) \), and we can write

\[
G(n, k) = G_1(n, k) \cup G_2(n, k).
\]

From the definition of \( G(n, k) \), it is obvious that the outdegree of every vertex in \( G(n, k) \) is 1. Since there are a finite number of vertices, then it follows that each component of \( G(n, k) \) contains a \( t \)-cycle. To each cycle vertex \( c \) in \( G(n, k) \), there is a tree attached to it denoted by \( T(n, k, c) \). The tree \( T(n, k, c) \) is one with vertex \( c \) as a root and all its other vertices are the non-cycle vertices \( b \) such that \( b^k \equiv c \pmod{n} \) for some positive integer \( i \), but \( b^{k-1} \) is not a cycle vertex in \( G(n, k) \). Cycles of length 1 are called fixed points. The vertices 0 and 1 are trivially fixed points.

### 1.4 Digraph Product

Consider a direct product digraph \( G(p_{e_1}^{e_1}, k) \times G(p_{e_2}^{e_2}, k) \times \cdots \times G(p_{e_r}^{e_r}, k) \). By the Chinese Remainder Theorem, there exists an isomorphism between \( G(n, k) \) and \( G(p_{e_1}^{e_1}, k) \times G(p_{e_2}^{e_2}, k) \times \cdots \times G(p_{e_r}^{e_r}, k) \) given by \( a \mapsto (a_1, a_2, \ldots, a_r) \), where \( a \equiv a_i \pmod{p_i^{e_i}} \) for all \( i \) such that \( 1 \leq i \leq r \). In otherwords, we have

\[
G(n, k) \cong G(p_{e_1}^{e_1}, k) \times G(p_{e_2}^{e_2}, k) \times \cdots \times G(p_{e_r}^{e_r}, k), \tag{1.4.1}
\]

and we say that a digraph \( G(n, k) \) can be factorized into a direct product of digraphs \( G(p_{e_i}^{e_i}, k) \) for all \( i \) such that \( 1 \leq i \leq r \). For \( a = (a_1, a_2, \ldots, a_r) \), we define \( a^k = (a_1, a_2, \ldots, a_r)^k = (a_1^k, a_2^k, \ldots, a_r^k) \).

The factorization of \( G(n, k) \) as (1.4.1) was first proved and studied by L. Somer and M. Krížek in [38]. This technique not only does it allows to reduce problems in \( G(n, k) \) to problems in \( G(p_{e_i}^{e_i}, k) \), which are relatively easier to handle, but it also provide a deeper insight into the structure of \( G(n, k) \). In this section, we state some fundamental results, mainly due to L. Somer and
M. Krížek [38], J. Kramer-Miller [19], and G. Deng and P. Yuan [12], to be used throughout the thesis.

**Lemma 1.4.1** (Theorem 6.7, [38]). A vertex \( c = (c_1, c_2, \ldots, c_r) \) is a cycle vertex in \( G(n, k) \) if and only if \( c_i \) is a cycle vertex in \( G(p_i^k, k) \) for all \( i \).

**Lemma 1.4.2** (Lemma 7, [19]). If \( a = (a_1, a_2, \ldots, a_r) \) and \( b = (b_1, b_2, \ldots, b_r) \) are vertices in the same cycle in \( G(n, k) \), then \( a_i \) and \( b_i \) are in the same cycle in \( G(p_i^k, k) \) for all \( i \).

Suppose \( n_1 \) and \( n_2 \) are relatively prime integers.

**Lemma 1.4.3** (Lemma 1, [19]). Let \( C(n_i, k) \) be a component of \( G(n_i, k) \) containing a \( t_i \)-cycle, for \( i = 1, 2 \). Then \( C(n_1, k) \times C(n_2, k) \) is a subdigraph of \( G(n_1, k) \times G(n_2, k) \) consisting of \( \gcd(t_1, t_2) \)-components each having cycles of length \( \text{lcm}(t_1, t_2) \).

**Theorem 1.4.4** (Theorem 6.8, [38]). Let \( J(n_i, k) \) be a union of components of \( G(n_i, k) \), for \( i = 1, 2 \). Then \( J(n_1, k) \times J(n_2, k) \) is a union of components of \( G(n_1, k) \times G(n_2, k) \). Moreover, if \( J(n_2, k) = \bigcup_{i=1}^{m} J_i(n_2, k) \), where each \( J_i(n_2, k) \) is a component of \( G(n_2, k) \), then \( J(n_1, k) \times J(n_2, k) = \bigcup_{i=1}^{m} J(n_1, k) \times J_i(n_2, k) \), where the union is disjoint.

Recall that the **indegree** of a vertex in a digraph is defined as the number of directed edges coming into it. In the context of a digraph \( G(n, k) \), we define the indegree of a vertex as follows:

**Definition 1.4.5.** The **indegree** of a vertex \( b \) in \( G(n, k) \), denoted by \( \text{indeg}^n_k(b) \), is the number of incongruent solutions of the congruence \( x^k \equiv b \pmod{n} \).

**Definition 1.4.6.** The **height** of a vertex \( a \) in \( G(n, k) \), denoted by \( h(a) \), is the least non-negative integer \( j \) such that \( a^{kj} \) is a cycle vertex in \( G(n, k) \). If \( C \) is a component of \( G(n, k) \), we define \( h(C) = \max_{a \in C} h(a) \).

**Definition 1.4.7** ([12]). Let \( O^m_t \) denote a component containing a \( t \)-cycle and is of height 1, and every vertex of positive indegree has indegree \( m \).
Lemma 1.4.8 (Lemma 5.5, [12]). We have $O_{t_1}^{m_1} \times O_{t_2}^{m_2} \cong \gcd(t_1, t_2)O_{\text{lcm}[t_1, t_2]}^{m_1 m_2}$.

Lemma 1.4.9 (Lemma 5.7, [12]). We have $O_m \times G \cong O_m \times H$ if and only if $G \cong H$, for any digraphs $G$ and $H$.

1.5 Indegree

There is a well known result in elementary number theory which says that the number of incongruent solutions of the congruence $f(x) \equiv 0 \pmod{n}$ is equal to the product of the number of incongruent solutions of the congruence $f(x) \equiv 0 \pmod{p_i^{e_i}}$ for all $i$ such that $1 \leq i \leq r$. Using this, we obtain

$$\text{indeg}_n^k(a) = \prod_{i=1}^{r} \text{indeg}_{p_i^{e_i}}^k(a_i), \quad (1.5.1)$$

for every vertex $a = (a_1, a_2, \ldots, a_r)$ in $G(n, k)$.

Theorem 1.5.1 (Lemma 2, [47]). Let $a$ be a vertex of positive indegree in $G_1(n, k)$. Then

$$\text{indeg}_n^k(a) = \prod_{i=1}^{r} \varepsilon_i \gcd(\lambda(p_i^{e_i}), k),$$

where $\varepsilon_i = 2$ if $2|k$ and $8|p_i^{e_i}$, and $\varepsilon_i = 1$ otherwise.

Explicit formulas for the indegree of vertices in $G(n, k)$ that are not relatively prime to $n$ was determined by L. Somer and M. Křížek in [38] and [37]. These formulas are crucial tools in proving our results.

Theorem 1.5.2 (Theorem 3.2, [37]). Let $b \neq 0$ be a vertex of positive indegree in $G_2(p^e, k)$ such that $p^\alpha || b$ for some $\alpha \geq 0$. Then $\alpha = kr$ for some integer $r \geq 1$, and \(\text{indeg}_{p^e}^k(b) = \delta p^{(k-1)r} \gcd(\lambda(p^{e-\alpha}), k),\) where $\delta = 2$ if $p = 2$ and $e - \alpha \geq 3$, and $\delta = 1$ otherwise.

Lemma 1.5.3 (Lemma 3.2, [38]). The indegree of 0 in $G_2(p^e, k)$ is given by \(\text{indeg}_{p^e}^k(0) = p^{e - \left\lceil \frac{e}{2} \right\rceil}\).
1.6 Cycles

We have seen that each component of $G(n,k)$ contains a cycle. The cycle structure of $G(n,k)$ was studied in-depth by B. Wilson in [47]. In his paper, he proved, among other results, various fundamental properties that are critical in the understanding of the cycles in $G(n,k)$.

Let $\lambda(n) = uv$, where $u$ is the largest divisor of $\lambda(n)$ relatively prime to $k$.

**Lemma 1.6.1** (Lemma 3, [47]). There is a $t$-cycle in $G_1(n,k)$ if and only if $t = \text{ord}_d(k)$ for some divisor $d$ of $u$.

**Lemma 1.6.2** (Corollary 6.2, [38]). Every cycle in $G_1(n,k)$ is a fixed point if and only if $k \equiv 1 \pmod{u}$.

**Lemma 1.6.3** (Theorem 4.1(iii), [37]). Every vertex in $G(n,k)$ is a cycle vertex if and only if $\gcd(\lambda(n), k) = 1$ and $n$ is square-free.

**Lemma 1.6.4** (Theorems 5.6 and 6.6, [38]). Let $A_t(G(n,k))$ denotes the number of $t$-cycles in $G(n,k)$. Then,

$$A_t(G(n,k)) = \frac{1}{t} \left[ \prod_{i=1}^{r} \left( \delta_i \gcd(\lambda(p_i^{e_i}), k^t - 1) + 1 \right) - \sum_{d|t, d \neq t} dA_d(G(n,k)) \right],$$

and

$$A_t(G_1(n,k)) = \frac{1}{t} \left[ \prod_{i=1}^{r} \delta_i \gcd(\lambda(p_i^{e_i}), k^t - 1) - \sum_{d|t, d \neq t} dA_d(G_1(n,k)) \right],$$

where $\delta_i = 2$ if $2|k^t - 1$ and $8|p_i^{e_i}$, and $\delta_i = 1$ otherwise.

**Lemma 1.6.5** (Lemma 3, [47]). A vertex $a \in G_1(n,k)$ is a cycle vertex if and only if $\text{ord}_a(a)|u$.

A fixed point in $G(n,k)$ is an isolated fixed point if its indegree is 1.

**Lemma 1.6.6** (Remark 8.3,[39]). The fixed point 0 is an isolated fixed point if and only if $n$ is square-free.

**Lemma 1.6.7** (Corollary 3, [47]). There are $\prod_{i=1}^{r} \gcd(\lambda(p_i^{e_i}), u)$ cycle vertices in $G_1(n,k)$.
1.7 Fundamental Constituents

Let $P$ be a subset of $Q = \{p_1, p_2, \ldots, p_r\}$. A fundamental constituent of $G(n, k)$, denoted by $G_P^*(n, k)$, is a subdigraph of $G(n, k)$ induced on the set of vertices which are multiples of $\prod_{p_i \in P} p_i$ and are relatively prime to all primes $p_j \in Q \setminus P$.

These subdigraphs of $G(n, k)$ were first defined by B. Wilson in [47]. In this section, we study the structure of $G_P^*(n, k)$ and state some basic results.

L. Somer and M. Krížek [39] proved that every fundamental constituent $G_P^*(n, k)$ of $G(n, k)$ can be written as

$$G_P^*(n, k) \cong G_1(n_1, k) \times T(n_2, k, 0), \tag{1.7.1}$$

where $n = n_1n_2$ with $\gcd(n_1, n_2) = 1$, and $p_i|n_2$ if and only if $p_i \in P$. In particular, $G_P^*(n, k) \cong G_1(n, k)$ and $G_Q^*(n, k) \cong T(n, k, 0)$. They also show that a digraph $G(n, k)$ can be expressed as a disjoint union of $G_P^*(n, k)$ where $P$ runs over all the subsets of $Q = \{p_1, p_2, \ldots, p_r\}$. More precisely,

$$G(n, k) = \bigcup_{P \subseteq Q} G_P^*(n, k), \tag{1.7.2}$$

where the union is disjoint.

Let $n = n_1n_2$, where $\gcd(n_1, n_2) = 1$, and $p_i|n_2$ if and only if $p_i \in P$. Using (1.7.1), the following results are obvious and follows immediately from Proposition 1.4.3 and Lemma 1.6.1.

**Proposition 1.7.1.** There is a $t$-cycle in $G_P^*(n, k) \cong G_1(n_1, k) \times T(n_2, k, 0)$ if and only if there is a $t$-cycle in $G_1(n_1, k)$.

**Proposition 1.7.2.** Let $G_P^*(n, k) \cong G_1(n_1, k) \times T(n_2, k, 0)$ be a fundamental constituent of $G(n, k)$. Then we have,

(a) $\mathcal{A}(G_P^*(n, k)) = \mathcal{A}(G_1(n_1, k)) = \mathcal{A}$, and

(b) $A_t(G_P^*(n, k)) = A_t(G_1(n_1, k))$ for all $t \in \mathcal{A}$. 

8
Section 1.8

An important property of a fundamental constituent, which further strengthens (1.7.2), is stated below:

**Theorem 1.7.3** (Theorem 6.1, [39]). *The trees attached to all cycle vertices in a fundamental constituent are isomorphic.*

The rest of this section is part of our work in [27].

Let \( l = m_1 m_2 \), where \( m_1 \) and \( m_2 \) are relatively prime integers with \( m_1 = \prod_{i=1}^{r} p_i^{e_i} \) and \( m_2 = \prod_{i=r+1}^{r+s} p_i^{e_i} \) as their respective prime factorizations. Consider the fundamental constituents \( G^*_{P_2}(m_1, k) \) and \( G^*_{Q_2}(m_2, k) \) of \( G(m_1, k) \) and \( G(m_2, k) \), respectively. Then using (1.7.1), we obtain

\[
G^*_{P_2}(m_1, k) \times G^*_{Q_2}(m_2, k) \cong G^*_{P_2 \cup Q_2}(l, k).
\]

In other words, the direct product of a fundamental constituent of \( G(m_1, k) \) and a fundamental constituent of \( G(m_2, k) \) results in a fundamental constituent of \( G(l, k) \). We also see that, if \( R = \{p_1, p_2, \ldots, p_r, p_{r+1}, \ldots, p_{r+s}\} \) and \( R_2 \subseteq R \), then

\[
G^*_{R_2}(l, k) \cong G^*_{R^i_2}(l_i, k) \times G^*_{R^j_2}(l_j, k),
\]

(1.7.3)

where \( R^i_2, R^j_2 \) are disjoint subsets of \( R_2 \) such that \( R^i_2 \cup R^j_2 = R_2 \), \( l_i l_j = l \) where \( \gcd(l_i, l_j) = 1 \), and \( R^i_2 = \{p_i \in R_2 : p_i \mid l_i\} \), \( R^j_2 = \{p_j \in R_2 : p_j \mid l_j\} \). In general, if \( n \) is factorized as (1.3.1) and \( P' = \{p_1, p_2, \ldots, p_s\} \) for any \( s \) such that \( 1 \leq s \leq r \), then we can write

\[
G^*_{P'}(n, k) \cong G^*_{\{p_1\}}(p_1, k) \times \cdots \times G^*_{\{p_s\}}(p_s, k) \times G^*_{\{p_{s+1}\}}(p_{s+1}, k) \times \cdots \times G^*_{\{p_r\}}(p_r, k).
\]

**Note 1.7.4.** If \( G^*_{Q_2}(m_1, k) \) is a fundamental constituent of \( G(m_1, k) \), then \( G^*_{Q_2}(l, k) \) is a fundamental constituent of \( G(l, k) \), and

\[
G^*_{Q_2}(l, k) \cong G^*_{Q_2}(m_1, k) \times G^*_{\emptyset}(m_2, k).
\]
1.8 Symmetry and Semiregularity

Definition 1.8.1 (Symmetry). [38] Let \( M \geq 2 \) be an integer. A digraph \( G(n,k) \) is symmetric of order \( M \) if its set of components can be partitioned into subsets of size \( M \), each containing \( M \) isomorphic components.

For example, the digraph \( G(39,3) \) in Figure 1.1 is symmetric of order 3.

![Figure 1.1: G(39,3)](image)

L. Somer and M. Krížek [38] characterized all integers \( n \) and \( k \) for which \( G(n,k) \) is symmetric of order \( M \). J. Kramer-Miller [19] proved another characterization of symmetric digraphs \( G(n,k) \) of order \( M \), when \( n \) is square-free, which G. Deng and P. Yuan [12] generalized it to any positive integer \( n \).

Theorem 1.8.2 (Theorem 3.5, [19]). Let \( n = pq_1q_2\cdots q_m \), where \( q_i \) and \( p \) are distinct odd primes. Suppose \( G(p,k) \) is not symmetric of order \( p \). Then \( G(n,k) \) is symmetric of order \( p \) if and only if both of the following conditions hold:

(a) \( \gcd(p-1,k) = 1 \).

(b) The set \( T = \{q_i : \gcd(q_i-1,k) = 1\} \) is non-empty, and for all \( x \in \mathbb{N} \) such that \( p \nmid A_x(G\left(\prod_{q_i \in T} q_i, k\right)) \), \( \operatorname{ord}_{p-1}(k)|x \).

There is also a very useful characterization, due to G. Deng and P. Yuan, for symmetric digraphs \( G(p^e,k) \) of order \( p \).

Theorem 1.8.3 (Theorem 4.1 [12]). Let \( p \) be an odd prime. Then \( G(p^e,k) \) is symmetric of order \( p \) if and only if \( \gcd(\lambda(p^e), k) = p^{e-1} \) and \( k \equiv 1 \pmod{p-1} \).
Definition 1.8.4 (Semiregularity, [35]). A digraph $G(n, k)$ is semiregular if there exists a positive integer $d$ such that the indegree of every vertex in $G(n, k)$ is either $d$ or 0.

From Theorem 1.5.1, it is clear that the subdigraph $G_1(n, k)$ is always semiregular. The semiregularity of $G_2(p^e, k)$ was characterized by L. Somer and M. Krížek [37] and we state their result below:

Theorem 1.8.5 (Theorem 4.4, [37]). Suppose $p$ is an odd prime.

(a) Let $p^a || k$ and $\gcd(p-1, k) = 1$. Then $G_2(p^e, k)$ is semiregular if and only if $1 \leq e \leq k + \alpha + 1$.

(b) Let $\gcd(p(p-1), k) = 1$. Then $G_2(p^e, k)$ is semiregular if and only if $1 \leq e \leq k + 1$.

(c) Let $\gcd(p-1, k) > 1$. Then $G_2(p^e, k)$ is semiregular if and only if $1 \leq e \leq k$.

Also, $G_2(2^e, k)$ is semiregular if and only if one of the following holds:

(a) $e \in \{1, 2, 3, 4, 6\}$ whenever $k = 2$.

(b) $1 \leq e \leq 9$ whenever $k = 4$.

(c) $1 \leq e \leq k + \alpha + 2$ whenever $k \geq 6$ and $2^a || k$.

Remark 1.8.6. (a) Let $2^a || k$, where $\alpha > 0$. If $T(2^e, k, 0)$ is not semiregular then $e > k + \alpha + 2$.

(b) Suppose $k$ is an odd integer. Then, looking at the indegrees of 0 and $2^k$ in $T(2^e, k, 0)$ one can inspect that $T(2^e, k, 0)$ is semiregular if and only if $1 \leq e \leq k + 1$.

Theorem 1.8.7 (Lemma 4.1, [12]). Let $p$ be an odd prime. Then $G(p^e, k)$ is semiregular if and only if $\gcd(p^{e-1}(p-1), k) = p^{e-1}$. 

11