KYUNGPOOK Math. J. 46(2006), 255-260

General Linear Group over a Ring of Integers of Modulo k

Juncheol Han
Department of Mathematics Education, Pusan National University, Pusan 609-735, Korea
e-mail : jchan@pusan.ac.kr

Abstract. Let m and k be any positive integers, let $\mathbb{Z}_k$ the ring of integers of modulo k, let $G_m(\mathbb{Z}_k)$ the group of all m by m nonsingular matrices over $\mathbb{Z}_k$ and let $\phi_m(k)$ the order of $G_m(\mathbb{Z}_k)$. In this paper, $\phi_m(k)$ can be computed by the following investigation: First, for any relatively prime positive integers s and t, $G_m(\mathbb{Z}_{st})$ is isomorphic to $G_m(\mathbb{Z}_s) \times G_m(\mathbb{Z}_t)$. Secondly, for any positive integer n and any prime p, $\phi_m(p^n) = p^{m^2} \cdot \phi_m(p^{n-1}) = p^{2m^2} \cdot \phi_m(p^{n-2}) = \cdots = p^{(n-1)m^2} \cdot \phi_m(p)$, and so $\phi_m(k) = \phi_m(p_1^{n_1}) \cdot \phi_m(p_2^{n_2}) \cdots \phi_m(p_s^{n_s})$ for the prime factorization of k, $k = p_1^{n_1} \cdot p_2^{n_2} \cdots p_s^{n_s}$.

1. Introduction

For any positive integers m and k, let $\mathbb{Z}$ (resp. $\mathbb{Z}_k = \{0, 1, \cdots, k-1\}$) be the ring of all integers (resp. the ring of integers under addition and multiplication modulo k) and let $M_m(\mathbb{Z})$ (resp. $M_m(\mathbb{Z}_k)$) the ring of all m by m matrices over $\mathbb{Z}$ (resp. the ring of all m by m matrices over $\mathbb{Z}_k$). Recall that the set of all m by m nonsingular matrices over $\mathbb{Z}$(resp. $\mathbb{Z}_k$) forms a group under the matrix multiplication (called the general linear group of degree m over $\mathbb{Z}$(resp. $\mathbb{Z}_k$)). We will denote this group by $G_m(\mathbb{Z})$ (resp. $G_m(\mathbb{Z}_k)$). Also we can note that the set of all m by m matrices in $M_m(\mathbb{Z})$ (resp. $M_m(\mathbb{Z}_k)$) with the determinant 1 forms a normal subgroup of $G_m(\mathbb{Z})$ (resp. $G_m(\mathbb{Z}_k)$) (called the special linear group of degree m over $\mathbb{Z}$ (resp. $\mathbb{Z}_k$)) and denoted by $S_m(\mathbb{Z})$ (resp. $S_m(\mathbb{Z}_k)$). Note that $A \in M_m(\mathbb{Z}_k)$ is nonsingular if and only if the determinant of $A \in M_m(\mathbb{Z}_k)$ is relatively prime to k. We will denote the determinant of $A \in M_m(\mathbb{Z})$ (or $M_m(\mathbb{Z}_k)$) by $|A|$.

Consider the following relation $\equiv_m$ defined on $M_m(\mathbb{Z})$: For any $A = [a_{ij}]$ and $B = [b_{ij}] \in M_m(\mathbb{Z})$, $A \equiv_m B(\text{mod } k)$ (we read this A is congruent to B modulo k) if $a_{ij} \equiv b_{ij}$ (modulo k) (i.e., $a_{ij} - b_{ij}$ is divided by k) for all $i,\ j = 1, 2, \cdots, m$. Observe that the congruence relation $\equiv_m$ is an equivalence relation on $M_m(\mathbb{Z})$ satisfying the following properties:

Received November 23, 2004.
2000 Mathematics Subject Classification: 11C20, 15A36.
Key words and phrases: $\mathbb{Z}_k$ (= the ring of integers of modulo k), general linear group of degree m over $\mathbb{Z}_k$, special linear group of degree m over $\mathbb{Z}_k$, congruence relation $\equiv_m$, order of group.
This work was supported by Pusan National University Research Grant.

(1) For any A, B, C and $D \in M_m(\mathbb{Z})$ such that $A \equiv_m B(\text{mod } k)$ and $C \equiv_m D(\text{mod } k)$, $A + C \equiv_m B + D(\text{mod } k)$.

(2) For any A, B, C and $D \in M_m(\mathbb{Z})$ such that $A \equiv_m B(\text{mod } k)$ and $C \equiv_m D(\text{mod } k)$, $AC \equiv_m BD(\text{mod } k)$. In particular, $A^s \equiv_m B^s(\text{mod } k)$ for all positive integers s.

(3) For any $A \in M_m(\mathbb{Z})$, there exists a unique element $A_0 \in M_m(\mathbb{Z}_k)$ such that $A \equiv_m A_0(\text{mod } k)$.

(4) For any $A \in G_m(\mathbb{Z})$, there exists a unique element $A_0 \in G_m(\mathbb{Z}_k)$ such that $A \equiv_m A_0(\text{mod } k)$.

We begin with the following Lemmas.

Lemma 1.1. *Let $A, B \in M_m(\mathbb{Z})$ such that $A \equiv_m B(\text{mod } k)$. Then $|A| \equiv |B|(\text{mod } k)$.*

Proof. It follows from the definition of the congruence $\equiv_m$. □

Note that the converse is not true.

Example 1. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{Z})$. Then $|A| \equiv |B|(\text{mod } 2)$, but A is not congruent to B modulo 2.

Throughout this paper, we will denote the greatest common divisor of any two positive integers s, t by $\gcd(s, t)$ (or simply (s, t)).

Lemma 1.2. *Let a and b be any integers and k be any positive integer. If $a \equiv b(\text{mod } k)$, then $(a, k) = (b, k)$.*

Proof. Clear. □

We can note that for any positive integers m and $n(n \geq 2)$ and any prime p, $G_m(\mathbb{Z}_{p^n})$ contains $G_m(\mathbb{Z}_{p^{n-1}})$ properly in the sense of set inclusion. Indeed, if $A \in G_m(\mathbb{Z}_{p^{n-1}})$, then $(|A|,\ p^{n-1}) = 1$, and so $(|A|,\ p^n) = 1$, which implies $A \in G_m(\mathbb{Z}_{p^n})$. For a diagonal matrix $D = [d_{ij}] \in G_m(\mathbb{Z}_{p^n})$ such that $d_{ii} = p^n$-1 for all $i = 1, 2, \cdots, m$, $D \notin G_m(\mathbb{Z}_{p^{n-1}})$. Hence $G_m(\mathbb{Z}_{p^n}) \supset G_m(\mathbb{Z}_{p^{n-1}})$, but $G_m(\mathbb{Z}_{p^n}) \neq G_m(\mathbb{Z}_{p^{n-1}})$. On the other hand, the subset $G_m(\mathbb{Z}_{p^{n-1}})$ of $G_m(\mathbb{Z}_{p^n})$ can not form a subgroup in $G_m(\mathbb{Z}_{p^n})$ by the following example.

Example 2. Let $A = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \in G_2(\mathbb{Z}_3)(\subset G_2(\mathbb{Z}_9))$. Then $A^3 = \begin{pmatrix} 8 & 7 \\ 0 & 1 \end{pmatrix} \in G_2(\mathbb{Z}_9) \setminus G_2(\mathbb{Z}_3)$. But $A^3 = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \in G_2(\mathbb{Z}_3)$.

Theorem 1.3. *Let m be any positive integer. If any two positive integers s and t are relatively prime, then $G_m(\mathbb{Z}_{st})$ is isomorphic to $G_m(\mathbb{Z}_s) \times G_m(\mathbb{Z}_t)$.*

Proof. Define $\psi : G_m(\mathbb{Z}_{st}) \to G_m(\mathbb{Z}_s) \times G_m(\mathbb{Z}_t)$ by $\psi(A) = (B, C)$ where $A \equiv_m B$ (mod s) and $A \equiv_m C$ (mod t). Then ψ is well-defined. Indeed, let $A \in G_m(\mathbb{Z}_{st})$

be arbitrary. Then $(|A|, st) = 1$. Since $(s,t) = 1$, $(|A|, s) = (|A|, t) = 1$. Since $A \equiv_m B \pmod{s}$ and $(|A|, s) = 1$, $(|B|, s) = 1$ by Lemma 1.1 and Lemma 1.2, and so $B \in G_m(\mathbb{Z}_s)$. Similarly, we can have $C \in G_m(\mathbb{Z}_t)$. By using the definition of congruence $\equiv_m$, we can easily show that ψ is a group homomorphism. Next, to prove ψ is onto, let $(B = [b_{ij}], C = [c_{ij}]) \in G_m(\mathbb{Z}_s) \times G_m(\mathbb{Z}_t)$ be arbitrary. Consider the following equations: for all $i, j = 1, \cdots, m$,

$$x_{ij} \equiv b_{ij} \pmod{s}, \quad x_{ij} \equiv c_{ij} \pmod{t}.$$

Since $(s,t) = 1$, the equations have the unique solution $a_{ij} \in M_m(\mathbb{Z}_{st})$ for all $i, j = 1, \cdots, m$ by the Chinese Remainder Theorem [1, page 75]. Let $A = [a_{ij}] \in M_m(\mathbb{Z}_{st})$. Then $A \equiv_m B \pmod{s}$ and $A \equiv_m C \pmod{t}$. Since $B \in G_m(\mathbb{Z}_s)$, $(|B|, s) = 1$. Since $A \equiv_m B \pmod{s}$, $(|A|, s) = 1$ by Lemma 1.2. By the similar argument, we can have $(|B|, t) = 1$. Since $(s,t) = 1$, $(|A|, st) = 1$, and so $A \in G_m(\mathbb{Z}_{st})$. Finally, we will show that ψ is one-one. Consider $ker(\psi) = \{A = [a_{ij}] \in G_m\mathbb{Z}_{st}) : A \equiv_m I_m \pmod{s}, A \equiv_m I_m \pmod{t}\}$. Let $A = [a_{ij}] \in ker(\psi)$. Then for all $i, j = 1, \cdots, m$, a_{ij} is the solution of following equations:

$$x_{ii} \equiv 1 \pmod{s}, \quad x_{ii} \equiv 1 \pmod{t};$$
$$x_{ij} \equiv 0 \pmod{s}, \quad x_{ij} \equiv 0 \pmod{t} \ (i \neq j).$$

On the other hand, by the Chinese Remainder Theorem both the equations have unique solutions in $\mathbb{Z}_{st}$, $x_{ii} = 1$ for all $i = 1, \cdots, m$ and $x_{ij} = 0$ for all $i, j = 1, \cdots, m$ and $i \neq j$. Hence $ker(\phi) = \{I_m\}$, and so ψ is one-one. Consequently, ψ is an isomorphism, and thus we have the result. □

Corollary 1.4. *Let m and k be any positive integers. If $p_1^{n_1} \cdot p_2^{n_2} \cdots p_s^{n_s}$ be the prime factorization of k, then $G_m(\mathbb{Z}_k)$ is isomorphic to $G_m(\mathbb{Z}_{p_1^{n_1}}) \times G_m(\mathbb{Z}_{p_2^{n_2}}) \times \cdots \times G_m(\mathbb{Z}_{p_s^{n_s}})$.*

Proof. It follows from Theorem 1.3 and induction on s. □

2. The order of $G_m(Z_k)$

Let $\phi_m(k)$ be the order of $G_m(\mathbb{Z}_k)$. In particular, if $m = 1$, then $\phi_1(k)$ is the *Euler-Phi* number of k, the number of elements of $\mathbb{Z}_k$ which are relatively prime to k. Recall that for any positive integer n and any prime p, $\phi_1(p^n) = p^n - p^{n-1} = p \cdot \phi_1(p^{n-1})$, and for any two relatively primes s and t, $\phi_1(st) = \phi_1(s) \cdot \phi_1(t)$. Let I_m (resp. $I_{m,k}$) be the identity of the group $G_m(\mathbb{Z})$ (resp. $G_m(\mathbb{Z}_k)$). If there is no confusion, we can let $I_m = I_{m,k}$ for the convenience of notation. From the properties of the congruence $\equiv_m$, we can have the following Theorem.

Theorem 2.1. *Let k be any positive integer and let $A \in M_m(\mathbb{Z})$ be arbitrary. If $|A|$ is relatively prime to k, then $A^{\phi_m(k)} \equiv_m I_m \pmod{k}$.*

Proof. For any $A \in M_m(\mathbb{Z})$, there exists a unique element $A_0 \in M_m(\mathbb{Z}_k)$ such that $A \equiv_m A_0 \pmod{k}$ by the property [3] of the congruence $\equiv_m$. By Lemma 1.1, $|A| \equiv |A_0| \pmod{k}$. Since $|A|$ is relatively prime to k, $A_0 \in G_m(\mathbb{Z}_k)$ by Lemma 1.2. Hence ${A_0}^{\phi_m(k)} \equiv_m I_m \pmod{k}$. Also by the property [2] of the congruence $\equiv_m$, $A^{\phi_m(k)} \equiv_m {A_0}^{\phi_m(k)} \pmod{k}$. Hence we have $A^{\phi_m(k)} \equiv_m I_m \pmod{k}$. □

Note that Theorem 2.1 extends *Euler's* Theorem stated as follows.

Euler's Theorem. Let a and k be any positive integers. If a is relatively prime to k, then $a^{\phi(k)} \equiv 1 \pmod{k}$.

Lemma 2.2. *Let m and n ($n \geq 2$) be any positive integers and let p be any prime. If $A \in G_m(\mathbb{Z}_{p^n})$ and $A_0 \in M_m(\mathbb{Z}_{p^{n-1}})$ such that $A \equiv_m A_0 \pmod{p^{n-1}}$, then $A_0 \in G_m(\mathbb{Z}_{p^{n-1}})$.*

Proof. If $A \in G_m(\mathbb{Z}_{p^n})$, then $(|A|, p^n) = 1$, and so $(|A|, p^{n-1}) = 1$. By Lemma 1.1 and Lemma 1.2, $(|A_0|, p^{n-1}) = 1$, and so $A_0 \in G_m(\mathbb{Z}_{p^{n-1}})$. □

Theorem 2.3. *Let m and n ($n \geq 2$) be any positive integers and let p be any prime. Then*

(1) *there exists a normal subgroup H of $G_m(\mathbb{Z}_{p^n})$ such that $G_m(\mathbb{Z}_{p^n})/H$ is isomorphic to $G_m(\mathbb{Z}_{p^{n-1}})$;*

(2) $\phi_m(p^n) = p^{m^2}\phi_m(p^{n-1})$;

(3) $\phi_m(p^n) = p^{m^2} \cdot \phi_m(p^{n-1}) = p^{2m^2} \cdot \phi_m(p^{n-2}) = \cdots = p^{(n-1)m^2} \cdot \phi_m(p)$, *where* $\phi_m(p) = (p^m - 1)(p^m - p) \cdots (p^m - p^{m-1})$.

Proof. (1) Define $\theta : G_m(\mathbb{Z}_{p^n}) \to G_m(\mathbb{Z}_{p^{n-1}})$ by $\theta(A) = A_0$, where $A \equiv_m A_0 \pmod{p^{n-1}}$ for all $A \in G_m(\mathbb{Z}_{p^n})$. Then θ is well-defined by Lemma 2.2. It is easy to show that θ is a group homomorphism. Next, we will show that θ is onto. Let $A_0 \in G_m(\mathbb{Z}_{p^{n-1}})$ be arbitrary. Then we can choose $A \in M_m(\mathbb{Z}_{p^n})$ such that $A \equiv_m A_0 \pmod{p^{n-1}}$. Indeed, for $A_0 \in G_m(\mathbb{Z}_{p^{n-1}})$ there exists $B \in M_m(\mathbb{Z})$ such that $B \equiv_m A_0 \pmod{p^{n-1}}$. By the property [3] of congruence $\equiv_m$, there exists $A \in M_m(p^n)$ such that $B \equiv_m A \pmod{p^n}$, and then $B \equiv_m A \pmod{p^{n-1}}$. Therefore $A \equiv_m A_0 \pmod{p^{n-1}}$. Since $A_0 \in G_m(\mathbb{Z}_{p^{n-1}})$, $(|A_0|, p^{n-1}) = 1$, and so $(|A_0|, p^n) = 1$. By Lemma 1.1 and Lemma 1.2, $(|A|, p^n) = 1$. Thus $A \in G_m(\mathbb{Z}_{p^n})$, which implies that θ is onto. Let $H = ker(\theta)$. Then $H = \{A = [a_{ij}] \in G_m(p^n) : a_{ii} \equiv 1 (\text{mod } p^{n-1})$ for all $i = 1, \cdots, m$, and $a_{ij} \equiv 0 \pmod{p^{n-1}}$ for all $i, j = 1, \cdots, m$ and $i \neq j\}$. By the First Isomorphism Theorem, we can have the result (1).

(2) Note that $A = [a_{ij}] \in ker(\theta)$ if and only if $a_{ii} = 1, 1 + 2p^{n-1}, \cdots, 1 + (p-1)p^{n-1}$ for all $i = 1, \cdots, m$ and $a_{ij} = 0, 0 + 2p^{n-1}, \cdots, 0 + (p-1)p^{n-1}$ for all $i, j = 1, \cdots, m$ and $i \neq j$. Hence the order of $H = ker(\theta)$ in (1) is p^{m^2} and so $\phi_m(p^n) =$ (the order of H)$\cdot$ $\phi_m(p^{n-1}) = p^{m^2} \cdot \phi_m(p^{n-1})$ by (1).

(3) By the similar argument given in the proof (1), $\phi_m(p^t) = p^{m^2}\phi_m(p^{t-1})$ for all $t = 2, \cdots, n$. It is easy to compute $\phi_m(p)$, $\phi_m(p) = (p^m - 1)(p^m - p) \cdots (p^m - p^{m-1})$. Thus we have the result. □

Corollary 2.4. *Let m and k be any positive integers. If $p_1^{n_1} \cdot p_2^{n_2} \cdots p_s^{n_s}$ be the prime factorization of k, then $\phi_m(k) = \phi_m(p_1^{n_1}) \cdot \phi_m(p_2^{n_2}) \cdots \phi_m(p_s^{n_s})$.*

Proof. It follows from Corollary 1.4 and Theorem 2.3. □

Example 3. $\phi_2(2) = 6$, $\phi_2(4) = 96$, $\phi_2(8) = 1536$, $\phi_2(3) = 48$, $\phi_2(27) = 314928$, $\cdots$, $\phi_3(2940) = 19,599,001,939,501,921,063,850,213,376,000$, etc.

Observe that for all $i = 1, 2, \cdots, m-1$, $\begin{pmatrix} G_i(\mathbb{Z}_k) & 0_1 \\ 0_2 & I \end{pmatrix}$ is a subgroup of $G_m(\mathbb{Z}_k)$ which is isomorphic to $G_i(\mathbb{Z}_k)$ where 0_1 is i by $m-i$ zero matrix, 0_2 is $m-i$ by i zero matrix and I is $m-i$ by $m-i$ identity matrix. Hence $\phi_i(k)$ is a divisor of $\phi_m(k)$. In fact, for the prime factorization of k, $p_1^{n_1} \cdot p_2^{n_2} \cdots p_s^{n_s}$, it is easily computed that for each $j = 1, 2, \cdots, s$,

$$\phi_m(p_j^{n_j}) = p_j^{(n_j-1)(m^2-i^2)} \frac{\phi_m(p_j)}{\phi_i(p_j)} \phi_i(p_j^{n_j}),$$

$$\frac{\phi_m(p_j)}{\phi_i(p_j)} = (p_j^m - 1)(p_j^m - p_j) \cdots (p_j^m - p_j^{m-i-1}) p_j^{i(m-i)} \phi_i(p_j).$$

Recall the special linear group of degree m over $\mathbb{Z}_k$, $S_m(\mathbb{Z}_k) = \{A \in G_m(\mathbb{Z}_k) : |A| \equiv 1 \pmod{k}\}$, is the normal subgroup of $G_m(\mathbb{Z}_k)$.

Lemma 2.5. *Let m and k be any positive integers. Then $G_m(\mathbb{Z}_k)/S_m(\mathbb{Z}_k)$ is isomorphic to $G_1(\mathbb{Z}_k)$.*

Proof. Define a map $\theta : G_m(\mathbb{Z}_k) \to G_1(\mathbb{Z}_k)$ by $\theta(A) = |A| (\text{mod } k)$. Then θ is a well-defined map. It is easy to show that θ is a group homomorphism and is onto. Note that $ker(\theta)$ is $S_m(\mathbb{Z}_k)$. By the First Isomorphism Theorem, $G_m(\mathbb{Z}_k)/S_m(\mathbb{Z}_k)$ is isomorphic to $G_1(\mathbb{Z}_k)$. □

From the above Lemma, we have that $|S_m(\mathbb{Z}_k)| = \frac{\phi_m(k)}{\phi_1(k)}$.

Corollary 2.6. *Let m and k be any positive integers and let $S_t = \{B \in G_m(\mathbb{Z}_k) : |B| \equiv t (\text{mod } k)\}$. Then $S_t = AS_m(\mathbb{Z}_k) = \{AC \in G_m(\mathbb{Z}_k) : C \in S_m(\mathbb{Z}_k)\}$ for any $A \in G_m(\mathbb{Z}_k)$ such that $|A| \equiv t (\text{mod } k)$, i.e., S_t is a left coset of $S_m(\mathbb{Z}_k)$ containing $A \in G_m(\mathbb{Z}_k)$.*

Proof. It is clear by Lemma 2.5. □

From the above Corollary, we have that for any s and $t \in G_1(\mathbb{Z}_k)$, $|S_s| = |S_t|$.

3. Some application to number theory

Recall that an integer g is said to be a primitive root modulo k if the order of g modulo k is $\phi_1(k)$. In [1, pp 172-173], the following theorem is given:

Theorem 3.1. *An integer $k \geq 2$ has a primitive root modulo k if and only if k is one of the following: 2, 4, p^t, $2p^t$, where p is an odd prime and t an arbitrary positive integer.*

Observe that g is a primitive root modulo k if and only if $G_1(\mathbb{Z}_k)$ is a cyclic group with a generator a where $g \equiv a \pmod{k}$. In this section, we will illustrate another proof of Theorem 3.1 by using the results obtained in section 1 and section 2.

Lemma 3.2. *$G_1(\mathbb{Z}_{2^n})$ is not a cyclic group for all positive integer $n \geq 3$.*

Proof. Let $(1 \neq) g \in G_1(\mathbb{Z}_{2^n})$ be arbitrary for all positive integer $n \geq 3$. Then $g = 1 + 4t$ or $g = -1 + 4t$ for some $k \geq 1$. It is easily computed that $g^{2^{n-2}} \equiv 1 \pmod{2^n}$. Since the order of $G_1(\mathbb{Z}_{p^n})$ is 2^{n-1}, $G_1(\mathbb{Z}_{p^n})$ is not cyclic for all positive integer $n \geq 3$. □

Lemma 3.3. *$G_1(\mathbb{Z}_{p^n})$ is a cyclic group for any odd prime p and all positive integer n.*

Proof. Let p be any odd prime. We will prove it by induction on n. When $n = 1$, $G_1(\mathbb{Z}_p)$ is clearly a cyclic group. Assume that $G_1(\mathbb{Z}_{p^{n-1}})$ is a cyclic group. The map $\theta : G_1(\mathbb{Z}_{p^n}) \to G_1(\mathbb{Z}_{p^{n-1}})$ defined by $\theta(a) = a_0$ where $a \equiv a_0 \pmod{p^{n-1}}$ for all $a \in G_1(\mathbb{Z}_{p^n})$ is a group homomorphism by the special case $m = 1$ in Theorem 2.3. Then by the First Isomorphism Theorem, $G_1(\mathbb{Z}_{p^n})/H$ is isomorphic to $G_1(\mathbb{Z}_{p^{n-1}})$ where $H = ker(\theta)$. By assumption, $G_1(\mathbb{Z}_{p^{n-1}})$ is cyclic and so $G_1(\mathbb{Z}_{p^n})/H$ is cyclic. Hence there exists a generator $gH \in G_1(\mathbb{Z}_{p^n})/H$, and so $g^{\phi(p^{n-1})} \in H$ but $g^t \notin H$ for all $t < g^{\phi(p^{n-1})}$. Observe that $g^{\phi(p^{n-1})}$ is not congruent to 1 mod p^n. Indeed, if $g^{\phi(p^{n-1})} \equiv 1 \pmod{p^n}$, then $g^{\phi(p^n)} \equiv g^{\phi(p^{n-1})} (\text{mod } p^n)$. Since g is relatively prime to p^n, $g^p \equiv 1 \pmod{p^n}$, which implies the order of $G_1(\mathbb{Z}_{p^n})/H$ is p, a contradiction. Therefore, $g^{\phi(p^{n-1})}$ is not congruent to 1 mod p^n. Since H is a cyclic group of order p, $g^{\phi(p^{n-1})}$ is a generator of H. Thus the order of $g \in G_1(\mathbb{Z}_{p^n})$ is $\phi(p^n)$, and so $G_1(\mathbb{Z}_{p^n})$ is a cyclic group. □

Lemma 3.4. *Let G and H be two finite cyclic groups of orders $|G|$ and $|H|$ respectively. Then $G \times H$ is a cyclic group if and only if $|G|$ and $|H|$ are relatively primes.*

Proof. Clear. □

Hence we can have the proof of the another version of Theorem 3.1 as follows:

Theorem 3.5. *For some positive integer k, $G_1(\mathbb{Z}_k)$ is a cyclic group if and only if k is one of the following: 2, 4, p^t, $2p^t$, where p is an odd prime and t an arbitrary positive integer.*

Proof. From the special case $m = 1$ in Corollary 1.4, we have that if $p_1^{n_1} \cdot p_2^{n_2} \cdots p_s^{n_s}$ is the prime factorization of any positive integer k, then $G_1(\mathbb{Z}_k)$ is isomorphic to $G_1(\mathbb{Z}_{p_1^{n_1}}) \times G_1(\mathbb{Z}_{p_2^{n_2}}) \times \cdots \times G_1(\mathbb{Z}_{p_s^{n_s}})$. Hence it follows from Lemma 3.2, Lemma 3.3 and Lemma 3.4. □

Acknowledgements. The author thanks Professor J. K. Park at Pusan National University for reading this paper and helpful suggestions.

References

[1] R. Kumanduri and C. Romero, Number Theory with Computer Applications, Prentice Hall, New Jersey, INC, 1998.