Filomat 36:3 (2022), 715–720
https://doi.org/10.2298/FIL2203715D

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

An Association between Digraphs and Rings

Hamza Daoub[a], Osama Shafah[b], Aleksandar Lipkovski[c]

[a]*Department of Mathematics, Faculty of Science, Zawia University, Libya*
[b]*Department of Mathematics, Faculty of Science, Sabratha University, Libya*
[c]*Faculty of Mathematics, University of Belgrade, Serbia*

Abstract. In the present article, we are going to highlight the relation between different digraphs (cycles) of finite commutative ring $\mathbb{Z}_n$ for a natural number n, under the map $(a, b) \mapsto (a + b, ab)$. The algorithm, which is used to perform the calculations, has been built in MATLAB®.

1. Introduction

The association between graphs and rings, such as unitary Cayley graph and zero divisor graph, have been studied for long time by variety of researchers. However, here we are following a different association, presented by A. Lipkovski in [1]. In the present paper the finite commutative ring $\mathbb{Z}_n$ is chosen to work on. In the ring of integers $\mathbb{Z}$, the set of multiples of an integer n forms an ideal, usually denoted by $n\mathbb{Z}$. The ring $\mathbb{Z}_n$ is the quotient ring of $\mathbb{Z}$ modulo the ideal $n\mathbb{Z}$, that is, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

We usually consider $\mathbb{Z}_n$ as consisting of $0, 1, \ldots, n-1$ with addition and multiplication modulo n. When there is no confusion, we will denote the element $[a]$ in $\mathbb{Z}_n$ by just a, and will consider the set of classes $\{0, 1, \ldots, n-1\}$ as a set of numbers (residues) in $\mathbb{Z}$.

Let n be a natural number. Define the mapping $\varphi : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$ by $\varphi(a, b) = (a + b, ab)$. Likely, this mapping reflects the structure of $\mathbb{Z}_n$. Since $\mathbb{Z}_n$ is finite, so one can interpret φ as finite digraph $G_n = G(\mathbb{Z}_n)$ with vertices $\mathbb{Z}_n \times \mathbb{Z}_n$ and arrows defined by φ.

The characteristic of the residue class ring $\mathbb{Z}_n$, which contains n elements, is n. Therefore, if n is not a prime, then $\mathbb{Z}_n$ has zero divisors and $\mathbb{Z}_n[x]$ is not a unique factorization ring (if $ab = 0$, $a \neq 0$, $b \neq 0$, then $(x - a)(x - b) = x[x - (a + b)]$ are two distinct non-associated factorizations of $x^2 - (a + b)x + ab$). However, if $\mathbb{Z}_n$ is a domain, then it must be a field. so that $\mathbb{Z}_n[x]$ is a UFD.

Few graphs $G_n = G(\mathbb{Z}_n)$ can be explicitly drawn as we can see in Figures 1, 2. One can notice some interesting properties of those graphs, such as, degrees of vertices and presence of cycles.

2020 *Mathematics Subject Classification*. Primary 11T99; Secondary 05C90
Keywords. finite graphs, finite rings, symmetric polynomials
Received: 14 May 2012; Accepted: 11 June 2013
Communicated by Miroslav Ćirić
Research supported by Ministry of Education, Science and Technological Research of Republic of Serbia, grant no. OI 174020
Email addresses: h.daoub@zu.edu.ly (Hamza Daoub), Osama.shafah@sabu.edu.ly (Osama Shafah), acal@matf.bg.ac.rs (Aleksandar Lipkovski)

2. Basic Notations and Properties

2.1. Degrees and Vertices:

In this work, we consider the degrees of vertices in $G(\mathbb{Z}_n)$. As usual, the outgoing (incoming) degree of a vertex (a, b) is the number of arrows going out (coming in) this vertex. Since G is a function, so it is clear that the outgoing degree of each vertex is one. One might ask what the incoming degree of the vertex (a, b) is. As it was shown in [1], the incoming degree of (a, b) equals the number of different roots of $x^2 - ax + b$.

Definition 2.1. *Let G be any digraph. A **walk** of length k in G is a sequence of vertices $v_0, v_1, ..., v_{k-1}$ of G such that for each $i = 1, 2, ..., k$, the edge e_i has tail v_{i-1} and head v_i. A walk is **closed** if $v_0 = v_{k-1}$. A **path** in G is a walk in which all the vertices are distinct.*

Note that a **cycle** is a closed walk, where $v_0 = v_{k-1}$ and the vertices $v_0, v_1, ..., v_{k-1}$ are distinct from each other, thus the definition of length is still applicable.

In this article, the sequence

$$(a_1, b_1) \to (a_2, b_2) \to ... \to (a_k, b_k)$$

of arrows in G defines a cycle of length k (or k-cycle) if $(a_k + b_k, a_k b_k) = (a_1, b_1)$, and $(a_i + b_i, a_i b_i) \neq (a_j, b_j)$ for all $j \leq i < k$. In addition, $\overrightarrow{C_k}$ will refer to directed cycle with vertices $0, 1, ..., k-1$.

In the Figure 1, we notice that there are cycles of length one; this holds for the vertices $(a_i, 0)$ for all $1 \leq i \leq k$. More precisely, there are exactly n cycles of length 1 in $G(\mathbb{Z}_n)$.

2.2. Related Properties:

A homomorphism of G to H, is a mapping $f : V(G) \to V(H)$ from G to H, such that it preserves edges, that is, if for any edge (u, v) of G, $(f(u), f(v))$ is an edge of H. We write simply $G \to H$.

If f is any homomorphism of G to H, then the digraph with vertices $f(v), v \in V(G)$, and edges $f(v)f(w), vw \in E(G)$ is a homomorphic image of G. Note that $f(G)$ is a subgraph of H, and that $f : G \to f(G)$ is a surjective homomorphism.

In particular, homomorphisms of G to H map paths in G to walks in H, and hence do not increase distance (the minimum length of paths connecting two vertices).

Proposition 2.1. *Let G and H be digraphs, and $f : G \to H$ a homomorphism. If $v_1, v_2, ..., v_{k-1}$ is a walk in G, then $f(v_0), f(v_1), ..., f(v_{k-1})$ is a walk in H, of the same length ([5]).*

Corollary 2.1. *A mapping $f : V(\overrightarrow{C_k}) \to V(G)$ is a homomorphism of $\overrightarrow{C_k}$ to G if and only if $f(1), f(2), ..., f(k)$ is a cycle in G.*

Observe that a set of vertices is independent in G if it contains no pair of adjacent vertices. In terms of the associated partition, we have the following condition. A given digraph G satisfies $G \to \overrightarrow{C_k}$ if and only if the vertices of G can be partitioned into k independent sets $S_0, S_1, ..., S_{k-1}$ so that each edge of G goes from S_i to S_{i+1} for some $i = 0, 1, ..., k-1$ (with addition modulo k).

Recalling that a cycle is a homomorphic image of a cycle, we can reformulate the last result as follows.

Corollary 2.2. *A digraph G satisfies $G \to \overrightarrow{C_k}$ if and only if the length of every closed walk in G is divisible by k.*

3. Further Properties

Theorem 3.1. *$f = \{([a]_n, [a]_m) \in \mathbb{Z}_n \times \mathbb{Z}_m \mid a \in \mathbb{Z}\}$ is a function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ iff $m \mid n$.*

Proof. See [3] page 89. □

Let m and k be relatively prime numbers, such that $n = m \cdot k, m < k$. Define a map

$$h_1 : \mathbb{Z}_n \to \mathbb{Z}_m$$

that maps representatives $0 \le a < n$ in $\mathbb{Z}_n$ to ($a \bmod m$) in $\mathbb{Z}_m$. Since m divides n, then h_1 is a homomorphism. Moreover, $kerh_1 = m\mathbb{Z}_n < \mathbb{Z}_n$, and $| kerh_1 |= k$.

Similarly, the same holds for $h_2 : \mathbb{Z}_n \to \mathbb{Z}_k$.

Observe that mappings h_1 and h_2 induce mappings of corresponding graphs, which will be denoted again by h_1 and h_2.

We will denote the longest cycle in the digraph $G(\mathbb{Z}_n)$ by $\overrightarrow{C_{l_n}}$, and all our discussion later will be based on the construction of h_1 and h_2. Furthermore, we will refer to $\mathbb{Z}_n$, $\mathbb{Z}_m$ and $\mathbb{Z}_k$ as sets of natural numbers.

Proposition 3.1. *Let $\overrightarrow{C_{l_n}}$ and $\overrightarrow{C_{l_m}}$ be two directed cycles in $G(\mathbb{Z}_n)$ and $G(\mathbb{Z}_m)$ respectively. If $\overrightarrow{C_{l_n}} \mapsto \overrightarrow{C_{l_m}}$ then we have that l_m divides l_n.*

Proof. Suppose that $\overrightarrow{C_{l_n}}$ is a s-cycle; that is,

$$(a_1, b_1) \to (a_2, b_2) \to \dots \to (a_s, b_s).$$

Since h_1 is a homomorphism, then

$$(h_1(a_1), h_1(b_1)) \to (h_1(a_2), h_1(b_2)) \to \dots \to (h_1(a_s), h_1(b_s))$$

is a cycle in $G(\mathbb{Z}_m)$, and

$$\begin{aligned} (h_1(a_1), h_1(b_1)) &= (h_1(a_s + b_s), h_1(a_s.b_s)) \\ &= (h_1(a_s) + h_1(b_s), h_1(a_s).h_1(b_s)) \end{aligned} \tag{1}$$

Since h_1 connects k elements in $\mathbb{Z}_n$ into every element $a \in \mathbb{Z}_m$, so that gives us two cases:

1. If $(h_1(a_1), h_1(b_1)) = (h_1(a_2), h_1(b_2))$. Then by (1), this process will be repeated for all $(h_1(a_i), h_1(b_i))$, $i = 2, \dots, s$. Thus $l_m = 1$ and $l_n = s \cdot l_m$.
2. If $(h_1(a_1), h_1(b_1)) = (h_1(a_j), h_1(b_j))$, for some $2 < j < s$. Then $(h_1(a_i), h_1(b_i)), i < j$ are all different. So according to (1) $l_n = t \cdot l_m$, for $1 \le t < s$. Hence l_n is divisible by l_m.

□

If we suppose that $\alpha \mid \beta$, $\alpha \neq 1$ (α might equal to β), then it is not proved yet that the maps f_1 and f_2 send the longest cycle $\overrightarrow{C}_\gamma$ in $G(Z_n)$ to longest cycles $\overrightarrow{C}_\alpha$ and $\overrightarrow{C}_\beta$ in $G(Z_p)$ and $G(Z_q)$ respectively. Because the cycles in $G(Z_p)$ and $G(Z_q)$ which are smaller than $\overrightarrow{C}_\alpha$ and $\overrightarrow{C}_\beta$ might have a pre-image which is a cycle with length longer than the pre-image of $\overrightarrow{C}_\alpha$ and $\overrightarrow{C}_\beta$ themselves. For instance, in $G(Z_47)$ the longest cycle is $\overrightarrow{C}_{12}$, and in $G(Z_11)$ the longest cycle is $\overrightarrow{C}_6$. While in $G(Z_517)$ the longest cycle is $\overrightarrow{C}_{30}$. Because there is a cycle $\overrightarrow{C}_{10}$ in $G(Z_47)$ that has a pre-image with $\overrightarrow{C}_6$ in $G(Z_517)$; that is exactly a multiple of these two. The computer calculations show that for n from 1 to 200 this exception case does not exist. However, if cycles $\overrightarrow{C}_\epsilon$ and $\overrightarrow{C}_\theta$ in $G(Z_p)$ and $G(Z_q)$ respectively are divisors of $\overrightarrow{C}_\alpha$ and $\overrightarrow{C}_\beta$ or they are loops, so the case like in $G(Z_517)$ can not happen again. Therefore, $1 < \epsilon < \alpha$, $1 < \theta < \beta$, and $\epsilon \mid \alpha$, $\theta \mid \beta$ is considered in the following results.

Proposition 3.2. *The maps h_1 and h_2 send the longest directed cycle $\overrightarrow{C_{l_n}}$ to the longest directed cycles $\overrightarrow{C_{l_m}}$, and $\overrightarrow{C_{l_k}}$ respectively.*

Proof. Suppose that $\overrightarrow{C}_{l_n}$ is the longest cycle in $G(\mathbb{Z}_n)$ of length s. Since h_1 is a homomorphism, then $h_1(\overrightarrow{C}_{l_n})$ is a cycle in $G(\mathbb{Z}_m)$ (by Corollary 1). According to Proposition 2, we have two cases:

1. If l_n is equal to l_m. Then, any other cycle $\overrightarrow{C}_{l_d}$ in $G(\mathbb{Z}_m)$ of length l_d, cannot be longer than l_m, because all cycles in the pre-image of this cycle will be longer than l_n.

2. If l_n is greater than l_m. Suppose that there is another cycle $\overrightarrow{C}_{l_d}$ in $G(\mathbb{Z}_m)$ of length l_d, such that $l_n > l_d > l_m$. In this case l_k cannot be 1, where l_k is the length of the longest cycle in $G(\mathbb{Z}_k)$. (If $l_k = 1$, then l_n must equal to l_m). Since h_1 is a homomorphism, then according to Corollary 1, any cycle in the pre-image of the cycle $\overrightarrow{C}_{l_d}$, let us say $\overrightarrow{C}_{l_r}$ has a length greater than or equal to l_d. We know that the length of $\overrightarrow{C}_{l_r}$ is a multiple of l_k as well. So the cycle $\overrightarrow{C}_{l_r}$ terminates exactly at one of the multiples of l_d and l_k. It is obvious that the least common multiple of l_d and l_k is greater than l_n. Thus, $\overrightarrow{C}_{l_r}$ has length longer than the longest cycle $\overrightarrow{C}_{l_n}$, which is a contradiction. Hence the proof follows.

□

Corollary 3.1. *All directed cycles $\overrightarrow{C_p}$, for all primes p are incomparable, i.e., $\overrightarrow{C_p} \to \overrightarrow{C_q}$ if and only if $p = q$.*

In the following we will use the so-called Chinese Remainder Theorem:

Theorem 3.2. *Let $n_1, \ldots, n_r \in \mathbb{N}$ be pairwise relatively prime numbers, i.e. $\gcd\left(n_i, n_j\right) = 1$ for $i \neq j$. Let $n = n_1 \cdot \cdots \cdot n_r$. Then the map*

$$\psi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}, [x] \mapsto ([x \bmod n_1], \ldots, [x \bmod n_r])$$

is an isomorphism of rings.

Proof. See e.g. [4]. □

Theorem 3.3. *Let $m, k \in \mathbb{N}$ be relatively prime numbers, i.e., $\gcd(m, k) = 1$. Let $n = m \cdot k$. Then, the length of the longest cycle $\overrightarrow{C_{l_n}}$ is the least common multiple of l_m and l_k, where l_m and l_k are the lengths of the longest cycles $\overrightarrow{C_{l_m}}$ and $\overrightarrow{C_{l_k}}$ respectively.*

Proof. We will use Theorem 1. and the argument below it. Consider that $\overrightarrow{C_{l_n}}$ is a s-cycle, that is

$$(a_1, b_1) \to (a_2, b_2) \to \ldots \to (a_s, b_s).$$

Then, $h_1(\overrightarrow{C_{l_n}})$ is a cycle in $G(\mathbb{Z}_m)$. Similarly, $h_2(\overrightarrow{C_{l_n}})$ is a cycle in $G(\mathbb{Z}_k)$. So according to Propositions 2 and 3, we have the following cases:

1. If $(a_1, b_1) \in \mathbb{Z}_m \times \mathbb{Z}_m \subset G(\mathbb{Z}_n)$. Then, both h_1 and h_2 send (a_1, b_1) to the same vertex, so that the cycle $\overrightarrow{C_{l_n}}$ must terminate at the first multiple of l_m and l_k, because (a_1, b_1) is a unique original vertex of $(h_1(a_1), h_1(b_1))$ and $(h_2(a_1), h_2(b_1))$.
2. If $(a_1, b_1) \notin \mathbb{Z}_m \times \mathbb{Z}_m$. Then, the map h_1 sends the element t in $\mathbb{Z}_n$ to element $t \bmod m$ in $\mathbb{Z}_m$. Similarly, the map h_2 sends the element t in $\mathbb{Z}_n$ to element $t \bmod k$ in $\mathbb{Z}_k$. Since m and k are two different modules, by Chinese Remainder Theorem, two different vertices $(h_1(a_1), h_1(b_1))$ and $(h_2(a_1), h_2(b_1))$ uniquely determine the original vertex (a_1, b_1). Thus the length of $\overrightarrow{C_{l_n}}$ terminates exactly at the first multiple of the lengths of $\overrightarrow{C_{l_m}}$ and $\overrightarrow{C_{l_k}}$. Hence the proof follows.

□

Theorem 3.4. *Let $p_1, \ldots, p_r \in \mathbb{N}$ be pairwise relatively prime numbers, i.e., $\gcd(p_i, p_j) = 1$ for $i \neq j$. Let $n = p_1 \cdot \ldots \cdot p_r$. Then the longest cycle $\overrightarrow{C_n}$ in $G(\mathbb{Z}_n)$ has a length $l_n = \operatorname{lcm}(l_{p_1}, l_{p_2}, \ldots, l_{p_r})$, where $l_{p_1}, l_{p_2}, \ldots, l_{p_r}$ are the lengths of the longest cycles in $G(\mathbb{Z}_{p_1})$, $G(\mathbb{Z}_{p_2})$, ..., $G(\mathbb{Z}_{p_r})$ respectively.*

Proof. The proof follows directly by Theorem 3 and the Chinese Remainder Theorem. □

Proposition 3.3. *The length of the longest cycle $\overrightarrow{C_{l_{p^m}}}$ can be either p^{m-1} or $\alpha \cdot l_p$ for some $\alpha > 1$, where l_p is the of the length of the longest cycle $\overrightarrow{C_{l_p}}$.*

Proof. Let p be a prime number, and $m > 1$ be any integer. The function $h : \mathbb{Z}_{p^m} \to \mathbb{Z}_p$ which is defined by $h(a) = a \bmod p$ is a homomorphism, and $kerh = p\mathbb{Z}_{p^m} < \mathbb{Z}_{p^m}$, where $\mid kerh \mid = p^{m-1}$.

Suppose that

$$(a_1, b_1) \to (a_2, b_2) \to ... \to (a_s, b_s)$$

is the longest cycle $\overrightarrow{C_{l_{p^m}}}$ in $G(\mathbb{Z}_{p^m})$. Therefore, if $b_1 \in kerh$, then $h(\overrightarrow{C_{l_{p^m}}})$ will be $(a, 0)$, $a = h(a_1) \in \mathbb{Z}_p$. Since then, $l_{p^m} = p^{m-1}$ (because p^{m-1} is the number of elements in $\mathbb{Z}_{p^m}$ which are congruent to $a \bmod p$), where l_{p^m} is the length of the cycle $\overrightarrow{C_{p^m}}$.

If $b_1 \notin kerh$, then a_1 won't be in $kerh$ neither. Thus we have a cycle $h(\overrightarrow{C_{p^m}})$ with length more that 1. According to theorem 3, we observe that the length of the cycle $h(\overrightarrow{C_{l_p}})$ divides l_{p^m}. Hence $l_{p^m} = \alpha l_p$ for some $\alpha > 1$. □

Note that, at the moment there is no way to determine the value of α in the second case. For instance, when $n = 5$, 5-cycle is the longest cycle in $G(\mathbb{Z}_{25})$. At the same time, 4-cycle is the longest cycle in $G(\mathbb{Z}_5)$. When $n = 11$, 30-cycle is the longest cycle in $G(\mathbb{Z}_{121})$. At the same time, 6-cycle is the longest cycle in $G(\mathbb{Z}_{11})$.

Let $n \in \mathbb{N}$ and $n = p_1^{n_1} p_2^{n_2} ... p_j^{n_j}$ be the decomposition of n into different primes. Then, according to Theorem 2, $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times ... \times \mathbb{Z}_{p^{n_j}}$.

Theorem 3.5. *Let $n \in \mathbb{N}$ and $n = p_1^{n_1} p_2^{n_2} ... p_r^{n_r}$ be the decomposition of n into primes, such that $p_i \neq p_j$ for $i \neq j$. Then, the longest cycle $\overrightarrow{C_n}$ of $G(\mathbb{Z}_n)$ has a length $l_n = \mathrm{lcm}(l_{p_1^{n_1}}, l_{p_2^{n_2}}, ..., l_{p_r^{n_r}})$, where $l_{p_1^{n_1}}$, $l_{p_2^{n_2}}$, ..., $l_{p_r^{n_r}}$ are the lengths of the longest cycles in $G(\mathbb{Z}_{p^{n_1}})$, $G(\mathbb{Z}_{p^{n_2}})$, ..., $G(\mathbb{Z}_{p^{n_r}})$ respectively.*

Proof. The proof comes by using Chinese Remainder Theorem, the preceding argument and Theorem 4. □

4. Graphs and Computer Calculations

Table 1 presents the computer calculations for n from 1 to 100. Some notations are used, such as Serial Number (S.NO), Longest cycle (L.C) and Number of cycles (NO.C). The calculations were performed on a PC using the MATLAB®

Here are two graphs $G(\mathbb{Z}_5)$ and $G(\mathbb{Z}_4)$. These graphs include 1-cycle, 2-cycle and 4-cycle. The components of these graphs are different in their number and appearance.

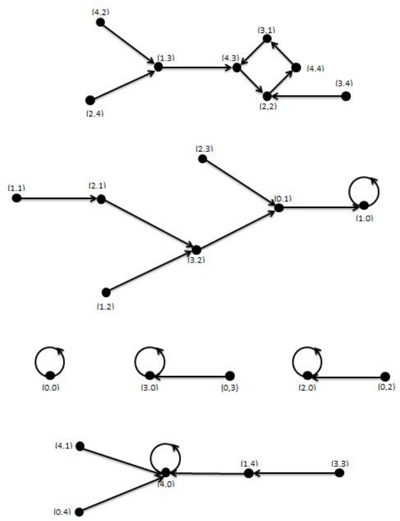

Figure 1: $G(\mathbb{Z}_5)$

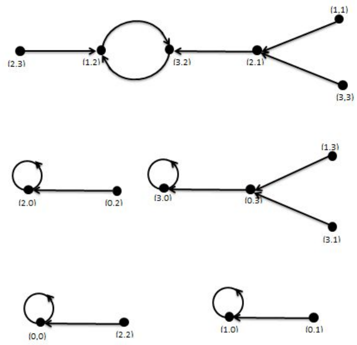

Figure 2: $G(\mathbb{Z}_4)$

References

[1] A. Lipkovski, Digraphs associated with rings and some integer functions, IX Congress of Mathematicians in Yugoslavia, Petrovac, May 22-27, 1995, Book of abstracts p. 32.

[2] A. Lipkovski, O. Shafah, H. Daoub, Vychislenie grafov konechnyh kolec, International Conference "Mathematical and informational technologies", Report 177, Vrnjacka Banja Serbia - Budva Montenegro, August 27-September 5, 2011.

[3] C. Lansky, Concepts in abstract algebra, Thomson Brooks/Col, USA, 2005.

[4] H. Delfs, H. Knebl, Introduction to Cryptography, Principles and Applications, (2nd edition), Springer-Verlag, Berlin Heidelberg, 2007.

[5] J. Ball, D. Welsh, Graphs and Homomorphisms, Oxford University Press, New York, 2004.

S. NO	L.C	NO.C	S. NO	L.C	NO.C	S. NO	L.C	NO.C	S. NO	L.C	NO.C
1	1	1	26	4	2	51	10	3	76	8	6
2	1	2	27	9	3	52	4	6	77	6	7
3	1	3	28	2	7	53	14	1	78	4	6
4	2	1	29	14	1	54	9	6	79	28	1
5	4	1	30	4	6	55	12	2	80	8	36
6	1	6	31	18	1	56	4	14	81	27	9
7	1	7	32	16	8	57	8	3	82	22	2
8	4	2	33	6	3	58	14	2	83	12	1
9	3	2	34	10	2	59	17	1	84	2	21
10	4	2	35	4	7	60	4	18	85	20	2
11	6	1	36	6	2	61	17	1	86	11	2
12	2	3	37	24	1	62	18	2	87	14	3
13	4	1	38	8	2	63	3	14	88	12	4
14	1	14	39	4	3	64	32	16	89	51	1
15	4	3	40	4	30	65	4	22	90	12	4
16	8	4	41	22	1	66	6	6	91	4	7
17	10	1	42	1	42	67	39	1	92	10	6
18	3	4	43	11	1	68	10	6	93	18	3
19	8	1	44	6	6	69	10	3	94	12	2
20	4	6	45	12	2	70	4	14	95	8	9
21	1	21	46	10	2	71	10	1	96	16	24
22	6	2	47	12	1	72	12	4	97	23	1
23	10	1	48	8	12	73	30	1	98	7	12
24	4	6	49	7	6	74	24	2	99	6	21
25	5	4	50	5	8	75	5	12	100	10	4

Table 1: The table of results