SOLUTIONS FOR THE 11$^{\text{TH}}$ INTERNATIONAL TOURNAMENT OF YOUNG MATHEMATICIANS

Team Bulgaria

Problem 7: Graphs of Finite Groups

Author: Ivan Durev, Plamen Ivanov

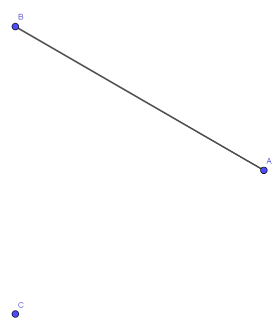
Abstract

We fully solved items 1. and 5. and partially item 4c.

Graphs of Finite Groups

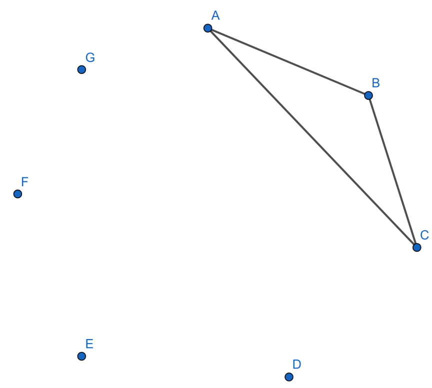
For simplicity we are going to use letters representing each graph's vertices. We will denote their meaning with M. An example, meaning that the letter A is the permutation 1432, part of S_4: M(A)=(1;4;3;2)

Item 1. *Solution.* Here is (Z_4), where $M(A) = 0, M(B) = 2, M(C) = 3$:
$B^2 = A$



Here is (D_4), where two of the symmetries are by the two diagonals of a square $ABCD$ and the other two are by the two lines defined by the two pairs of opposite sides.

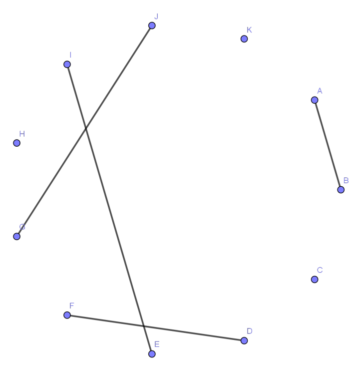
$$M(A) = rotate(90) \quad M(D) = symmetry(AC)$$
$$M(B) = rotate(180) \quad M(E) = symmetry(BD)$$
$$M(C) = rotate(270) \quad M(F) = symmetry(MN)$$
$$M(G) = symmetry(PQ)$$



Here is (A_4), where

$$\begin{array}{lll} M(A) = (1;3;4;2) & M(E) = (2;4;3;1) & M(I) = (4;1;3;2) \\ M(B) = (1;4;2;3) & M(F) = (3;1;2;4) & M(J) = (4;2;1;3) \\ M(C) = (2;1;4;3) & M(G) = (3;2;4;1) & M(K) = (4;3;2;1) \\ M(D) = (2;3;1;4) & M(H) = (3;4;1;2) & \end{array}$$

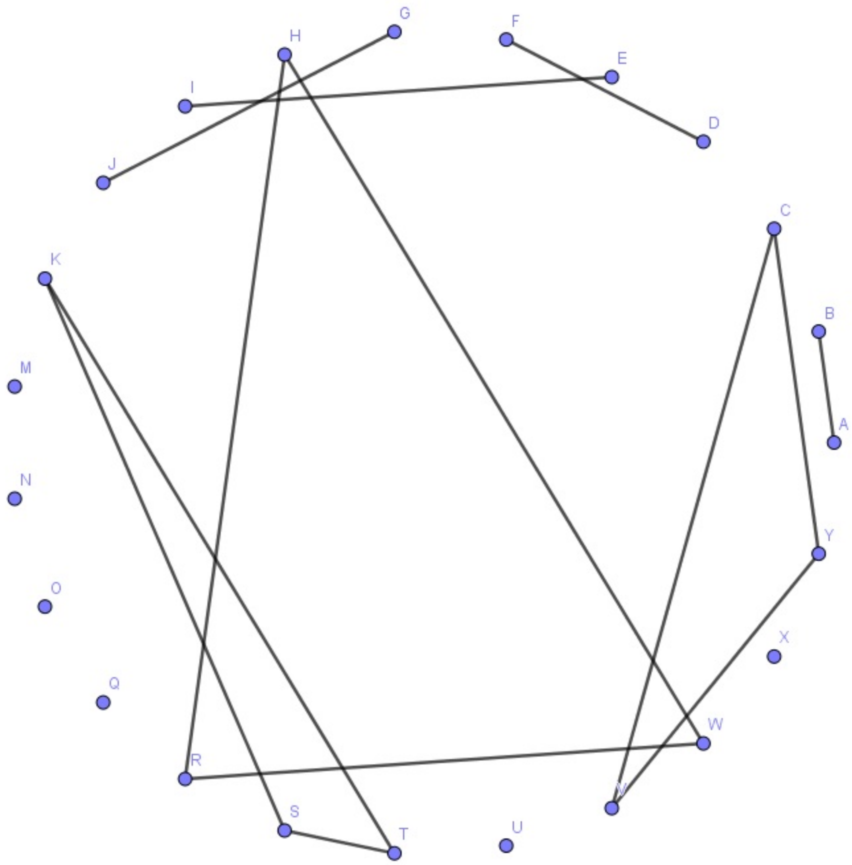
$$A^2 = B$$
$$D^2 = F$$
$$E^2 = I$$
$$G^2 = J$$



Here is (S_4), where

$$\begin{array}{ccc} M(A) = (1;3;4;2) & M(I) = (4;1;3;2) & M(S) = (2;4;1;3) \\ M(B) = (1;4;2;3) & M(J) = (4;2;1;3) & M(T) = (3;1;4;2) \\ M(C) = (2;1;4;3) & M(K) = (4;3;2;1) & M(U) = (3;2;1;4) \\ M(D) = (2;3;1;4) & M(M) = (1;2;4;3) & M(V) = (3;4;2;1) \\ M(E) = (2;4;3;1) & M(N) = (1;3;2;4) & M(W) = (4;1;2;3) \\ M(F) = (3;1;2;4) & M(O) = (1;4;3;2) & M(X) = (4;2;3;1) \\ M(G) = (3;2;4;1) & M(Q) = (2;1;3;4) & M(Y) = (4;3;1;2) \\ M(H) = (3;4;1;2) & M(R) = (2;3;4;1) & \end{array}$$

$$\begin{array}{ccc} A^2 = B & R^2 = H & T^2 = K \\ D^2 = F & R^3 = W & W^2 = H \\ E^2 = I & S^2 = K & Y^2 = C \\ G^2 = J & S^3 = T & Y^3 = V \\ & & V^2 = C \end{array} \qquad \blacksquare$$



Item 5. We are going to show the condition under which the item is held true:

$$\text{For } p\text{-prime: } (Z_p) \simeq K_{p-2} \cup \{0\} \iff p = 2^{2^n} + 1$$

Solution. Let $p = 2^{2l} + 1$ and p is a prime. Let k be the order of a modulo p, where $1 < a < p$. Obviously, $gcd(a;p) = 1$. From Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$.

Theorem 1. $k \mid p - 1$

Proof. Let us assume that the opposite is true and x be such a positive integer that: $kx < p-1 < k(x+1)$.

$$a^{kx} \equiv 1 \pmod{p}$$
$$a^{p-1} \equiv 1 \pmod{p} \text{ From } \textbf{Fermat's Little Theorem}$$
$$\implies a^{p-1} - a^{kx} \equiv 0 \pmod{p}$$
$$a^{kx}(a^{p-1-kx} - 1) \equiv 0 \pmod{p}$$
$$\implies a^{p-1-kx} \equiv 1 \pmod{p}$$

But $p-1-kx < k \implies$ Contradiction with the definition of order.

Thus, the theorem is proved and also analogically:

$k \mid y$ for every y, so that $a^y \equiv 1 \pmod{p}$

$\implies k \mid 2^{2^l}$
Let $k = 2^m$, where $m \in \mathbb{Z}$ and $m \geq 1$

$$a^k - 1 \equiv 0 \pmod{p}$$
$$(a^{2^m-1} - 1)(a^{2^m-1} + 1) \equiv 0 \pmod{p}$$

p divides only one of the two multipliers.

If $p \mid a^{2^m-1} - 1 \implies$ Contradiction with the definition of order.

If $p \mid a^{2^m-1} + 1 \implies a^{2^m-1} \equiv -1 \pmod{p}$

Therefore, for every number a there exists a power r such that: $a^r \equiv -1 \pmod{p}$, where $p = 2^{2^l} + 1$. Thus, every number is connected with $p-1$ and with all the other numbers except 0 and 1.
The " $\implies$ " direction is complete.

Let p be a prime but not of the aforementioned form.
Let's assume that all numbers from Z_p to some power have remainder -1 modulo p.

Then:

$$
\begin{aligned}
& 2^{2^l m} \equiv -1 \pmod p\text{, where } 2^l m \text{ is the least such number and } 2 \nmid m \\
& 2^l m < p - 1 \\
& 2^{2^{l+1} m} \equiv 1 \pmod p \\
\implies & 2^{l+1} m \text{ is the order of 2 modulo } p \\
& \text{Let } 2^{2^{l+1}} \equiv x \pmod p \\
& \text{Let } q \text{ be such a number that: } x^q \equiv -1 \pmod p \\
\implies & 2^{2^{l+2} q} \equiv 1 \pmod p \\
\text{From } \textbf{Theorem 1}\text{: } & 2^{l+1} m \mid 2^{l+2} q \\
\implies & m \mid q \implies 2^{l+1} m \mid 2^{l+1} q \\
\implies & 2^{l+1} q \equiv 1 \pmod p
\end{aligned}
$$

But that is a contradiction.

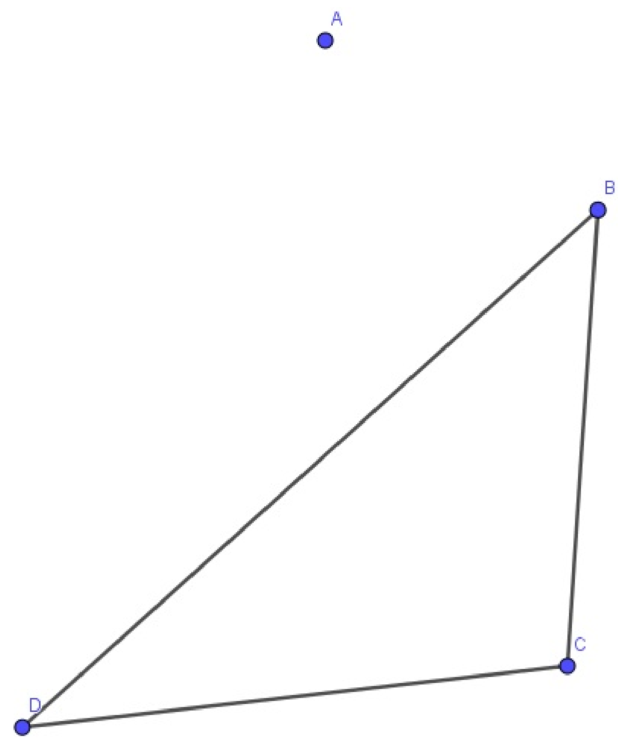
Therefore, the "$\Longleftarrow$" direction is complete. ■

Item 4c. *Solution.* We are going to show that Z_n is planar for every $n \leq 10 \cup 12$

The cases for Z_2 and Z_3 are trivial.

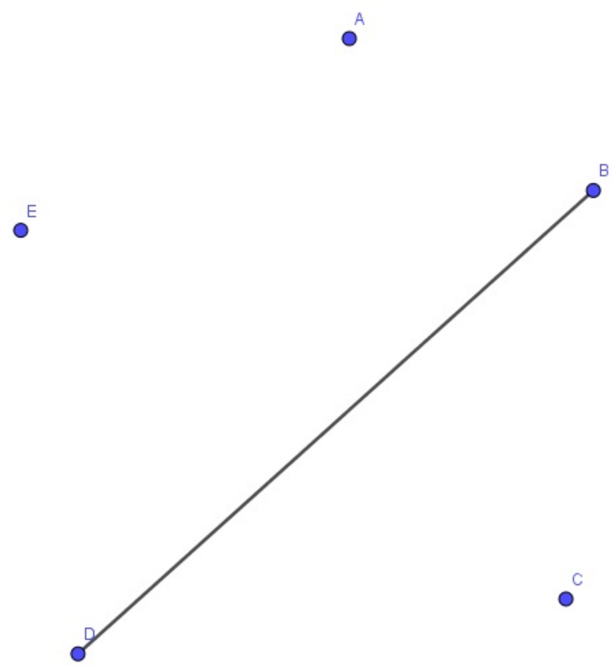
Numbers that aren't in the graph are simply not connected to any vertex.

Here is (Z_5), where



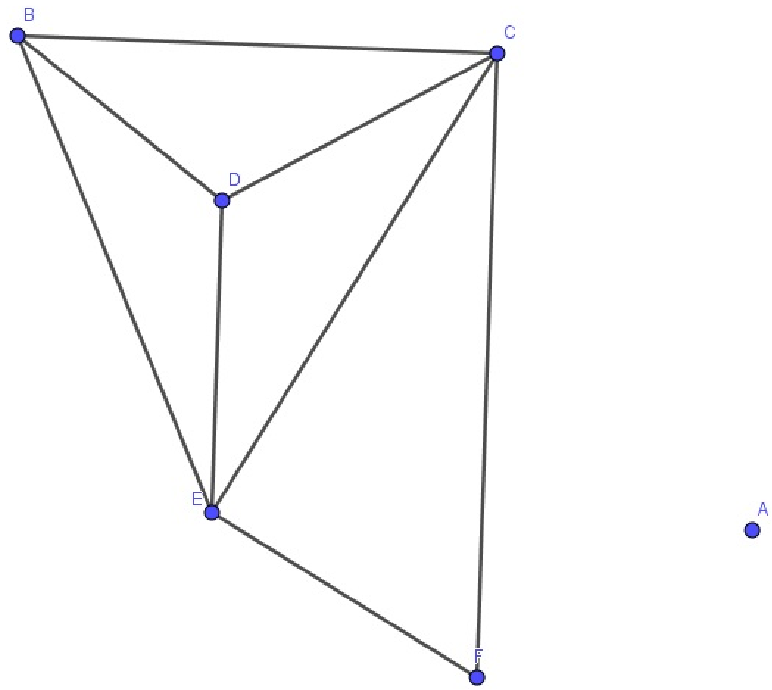
$$M(A) = 0$$
$$M(B) = 2$$
$$M(C) = 3$$
$$M(D) = 4$$

Here is (Z_6), where



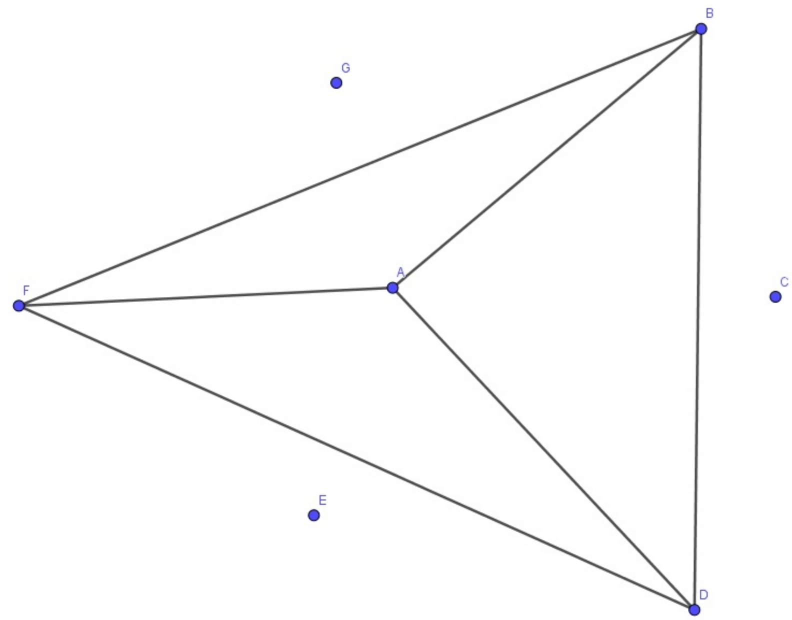
$$M(A) = 0$$
$$M(B) = 2$$
$$M(C) = 3$$
$$M(D) = 4$$
$$M(E) = 5$$

Here is (Z_7), where



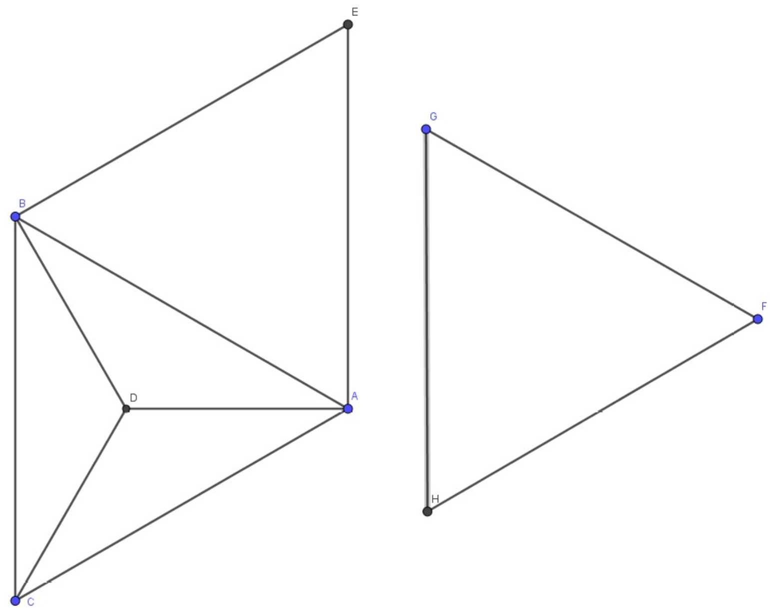
$$M(A) = 0 \quad M(D) = 4$$
$$M(B) = 2 \quad M(E) = 5$$
$$M(C) = 3 \quad M(F) = 6$$

Here is (Z_8), where



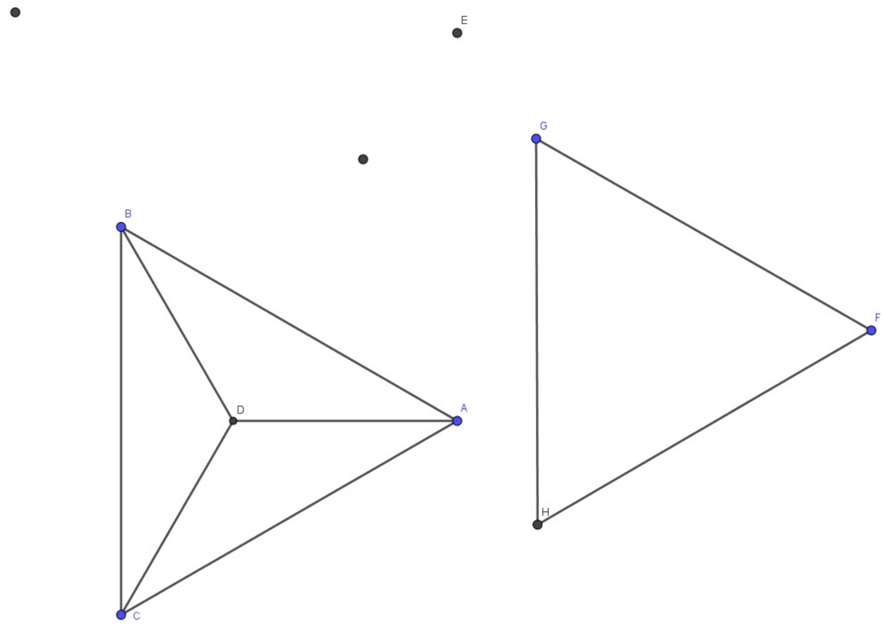
$$\begin{array}{ll} M(A) = 0 & \\ M(B) = 2 & M(E) = 5 \\ M(C) = 3 & M(F) = 6 \\ M(D) = 4 & M(G) = 7 \end{array}$$

Here is (Z_9), where



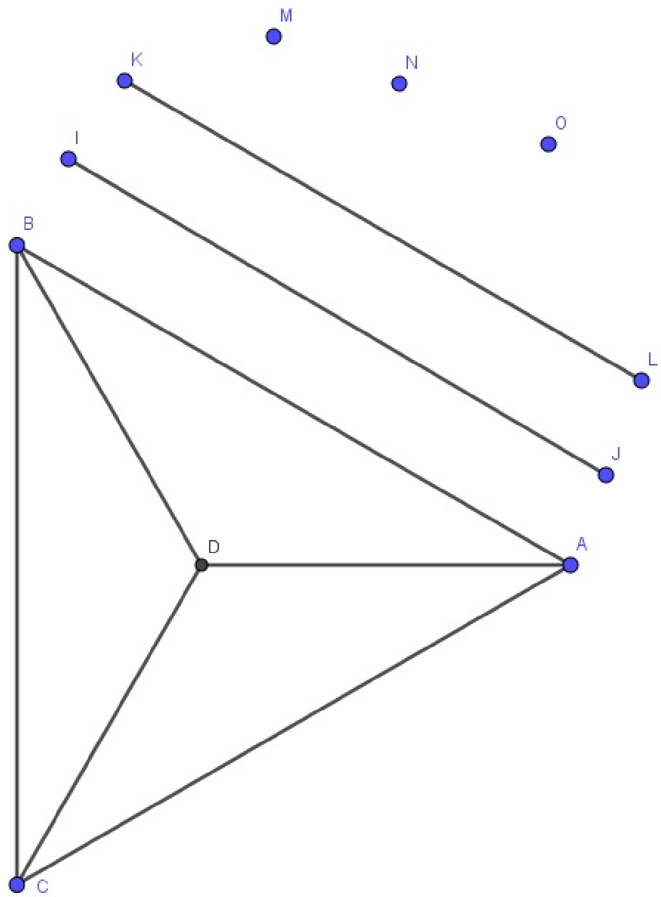
$$M(A) = 2 \quad M(E) = 8$$
$$M(B) = 5 \quad M(F) = 0$$
$$M(C) = 4 \quad M(G) = 3$$
$$M(D) = 7 \quad M(H) = 6$$

Here is (Z_{10}), where



$$
\begin{array}{ll}
M(A) = 2 & \\
M(B) = 4 & M(F) = 3 \\
M(C) = 6 & M(G) = 7 \\
M(D) = 8 & M(H) = 9 \\
M(E) = 0 &
\end{array}
$$

Here is (Z_{12}), where



$$M(A) = 2 \quad M(N) = 7$$
$$M(B) = 4 \quad M(O) = 11$$
$$M(C) = 8 \quad M(K) = 3$$
$$M(D) = 10 \quad M(L) = 9$$
$$M(M) = 5 \quad M(I) = 0$$
$$M(J) = 6$$

According to **Kuratowski's theorem** a graph is not planar if it contains K_5. We are first going to prove that (Z_n) contains K_5 for every $n > 20$. Let's consider the numbers $2, 4, 16, n-4$ and $n-2$, which are distinct for every $n > 20$.

$$
\begin{aligned}
&2^2 \equiv 4 \not\equiv 1 \pmod{n}\\
&2^4 \equiv 16 \not\equiv 1 \pmod{n}\\
&2^4 \equiv (n-4)^2 \not\equiv 1 \pmod{n}\\
&2^2 \equiv (n-2) \not\equiv 1 \pmod{n}\\
&4^2 \equiv 16 \not\equiv 1 \pmod{n}\\
&4^2 \equiv (n-4)^2 \not\equiv 1 \pmod{n}\\
&4 \equiv (n-2)^2 \not\equiv 1 \pmod{n}\\
&16 \equiv (n-4)^2 \not\equiv 1 \pmod{n}\\
&16 \equiv (n-2)^4 \not\equiv 1 \pmod{n}\\
&(n-4)^2 \equiv (n-2)^4 \not\equiv 1 \pmod{n}
\end{aligned}
$$

Neither of these remainders can be 1 for $n > 20$:

$$
\begin{aligned}
&16 \not\equiv 1 \pmod{n}\\
&(n-2)^2 \equiv n^2 - 4n + 4 \not\equiv 1 \pmod{n}\\
&(n-2)^4 = n^4 - 8n^3 + 24n^2 - 32n + 16 \not\equiv 1 \pmod{n}\\
&(n-4)^2 = n^2 - 8n + 16 \not\equiv 1 \pmod{n}
\end{aligned}
$$

Therefore, every graph Z_n, as defined in the problem, with more than 20 vertices is not planar. Now, we have to show that for $n = \{11, 13, 15, 16, 17, 18, 19, 20\}$ a subgraph K_5 exists.

n=11

$$
\begin{aligned}
&2^8 \equiv 3 \not\equiv 1 \pmod{n} && 3 \equiv 5^2 \not\equiv 1 \pmod{n}\\
&2^2 \equiv 4 \not\equiv 1 \pmod{n} && 3 \equiv 6^2 \not\equiv 1 \pmod{n}\\
&2^4 \equiv 5 \not\equiv 1 \pmod{n} && 4^2 \equiv 5 \not\equiv 1 \pmod{n}\\
&2^9 \equiv 6 \not\equiv 1 \pmod{n} && 4^2 \equiv 6^2 \not\equiv 1 \pmod{n}\\
&3 \equiv 4^4 \not\equiv 1 \pmod{n} && 5^2 \equiv 6^2 \not\equiv 1 \pmod{n}
\end{aligned}
$$

n=13

$$
\begin{aligned}
&2^4 \equiv 3 \not\equiv 1 \pmod{n} && 3 \equiv 6^8 \not\equiv 1 \pmod{n}\\
&2^2 \equiv 4 \not\equiv 1 \pmod{n} && 3^2 \equiv 7^4 \not\equiv 1 \pmod{n}\\
&2^5 \equiv 6 \not\equiv 1 \pmod{n} && 4^5 \equiv 6^2 \not\equiv 1 \pmod{n}\\
&2^{11} \equiv 7 \not\equiv 1 \pmod{n} && 4^{11} \equiv 7^2 \not\equiv 1 \pmod{n}\\
&3 \equiv 4^2 \not\equiv 1 \pmod{n} && 6^2 \equiv 7^2 \not\equiv 1 \pmod{n}
\end{aligned}
$$

n=14

$$
\begin{array}{ll}
2^2 \equiv 4 \not\equiv 1 \pmod{n} & 4^3 \equiv 8 \not\equiv 1 \pmod{n} \\
2^3 \equiv 6^2 \not\equiv 1 \pmod{n} & 4^2 \equiv 10^2 \not\equiv 1 \pmod{n} \\
2^3 \equiv 8 \not\equiv 1 \pmod{n} & 6^2 \equiv 8 \not\equiv 1 \pmod{n} \\
2 \equiv 10^2 \not\equiv 1 \pmod{n} & 6 \equiv 10^3 \not\equiv 1 \pmod{n} \\
4^3 \equiv 6^2 \not\equiv 1 \pmod{n} & 8 \equiv 10^6 \not\equiv 1 \pmod{n}
\end{array}
$$

n=15

$$
\begin{array}{ll}
2^2 \equiv 4 \not\equiv 1 \pmod{n} & 4 \equiv 8^2 \not\equiv 1 \pmod{n} \\
2^2 \equiv 7^2 \not\equiv 1 \pmod{n} & 4 \equiv 13^2 \not\equiv 1 \pmod{n} \\
2^3 \equiv 8 \not\equiv 1 \pmod{n} & 7^2 \equiv 8^2 \not\equiv 1 \pmod{n} \\
2^2 \equiv 13^2 \not\equiv 1 \pmod{n} & 7^2 \equiv 13^2 \not\equiv 1 \pmod{n} \\
4 \equiv 7^2 \not\equiv 1 \pmod{n} & 8^2 \equiv 13^2 \not\equiv 1 \pmod{n}
\end{array}
$$

n=16

$$
\begin{array}{ll}
0 \equiv 2^4 \not\equiv 1 \pmod{n} & 2^2 \equiv 6^2 \not\equiv 1 \pmod{n} \\
0 \equiv 4^2 \not\equiv 1 \pmod{n} & 2^3 \equiv 8 \not\equiv 1 \pmod{n} \\
0 \equiv 6^4 \not\equiv 1 \pmod{n} & 4 \equiv 6^2 \not\equiv 1 \pmod{n} \\
0 \equiv 8^2 \not\equiv 1 \pmod{n} & 4^3 \equiv 8^2 \not\equiv 1 \pmod{n} \\
2 \equiv 4^2 \not\equiv 1 \pmod{n} & 6^3 \equiv 8 \not\equiv 1 \pmod{n}
\end{array}
$$

n=17 From **Item 5.** we have proved that this graph contains K_15 and is, thus, not planar.

n=18

$$
\begin{array}{ll}
2^2 \equiv 4 \not\equiv 1 \pmod{n} & 4^3 \equiv 10 \not\equiv 1 \pmod{n} \\
2^3 \equiv 8 \not\equiv 1 \pmod{n} & 4^2 \equiv 14^2 \not\equiv 1 \pmod{n} \\
2^6 \equiv 10 \not\equiv 1 \pmod{n} & 8^2 \equiv 10 \not\equiv 1 \pmod{n} \\
2^5 \equiv 14 \not\equiv 1 \pmod{n} & 8 \equiv 14^3 \not\equiv 1 \pmod{n} \\
4^3 \equiv 8^2 \not\equiv 1 \pmod{n} & 10 \equiv 14^6 \not\equiv 1 \pmod{n}
\end{array}
$$

n=19

$$
\begin{array}{ll}
2^3 \equiv 3^3 \not\equiv 1 \pmod{n} & 3^4 \equiv 5 \not\equiv 1 \pmod{n} \\
2^2 \equiv 4 \not\equiv 1 \pmod{n} & 3^4 \equiv 6^5 \not\equiv 1 \pmod{n} \\
2^6 \equiv 5^6 \not\equiv 1 \pmod{n} & 4^5 \equiv 5^4 \not\equiv 1 \pmod{n} \\
2^{14} \equiv 6 \not\equiv 1 \pmod{n} & 4^3 \equiv 6^3 \not\equiv 1 \pmod{n} \\
3^6 \equiv 4^3 \not\equiv 1 \pmod{n} & 5^2 \equiv 6 \not\equiv 1 \pmod{n}
\end{array}
$$

n=20

$$\begin{array}{ll} 2^2 \equiv 4 \not\equiv 1 \pmod{n} & 4^3 \equiv 8^2 \not\equiv 1 \pmod{n} \\ 2^4 \equiv 6^2 \not\equiv 1 \pmod{n} & 4 \equiv 12^2 \not\equiv 1 \pmod{n} \\ 2^3 \equiv 8 \not\equiv 1 \pmod{n} & 6^2 \equiv 8^4 \not\equiv 1 \pmod{n} \\ 2^2 \equiv 12^2 \not\equiv 1 \pmod{n} & 6^2 \equiv 12^4 \not\equiv 1 \pmod{n} \\ 4^2 \equiv 6^2 \not\equiv 1 \pmod{n} & 8^2 \equiv 12^2 \not\equiv 1 \pmod{n} \end{array}$$

Therefore, every graph Z_n with $n > 12$ or $n = 11$ contains a subgraph K_5, because we can connect the described for each n numbers, and is, hence, not planar. ■