Divisibility graphs

Anne-Julie Bertinchamps Tia De Waha

Second Semestre 2021-2022

Supervisors:

- Antonella Perucca
- Emiliano Torti

FACULTY OF SCIENCE,
TECHNOLOGY
AND MEDICINE

1 Motivation

It is easy to know if a number is divisible by 2, by 3, by 5 or also by 10. There exist divisibility criteria with respect to different numbers, for example:

- A number is divisible by 2 if and only if its last digit is even. For instance, $4, 6, 8, 10, 12.345.678$ are divisible by 2.
- A number is divisible by 3 if the sum of its digits is divisible by 3.

  Example. $12 : 1+2 = 3$ thus 12 is divisible by 3.
  $1.273.843.095 :\ 1+2+7+3+8+4+3+0+9+5 = 42$, and $4+2 = 6$ thus 1.273.843.095 is divisible by3.
- A number is divisible by 5 if and only if its last digit is 0.

  Example. $10, 285, 15.938.215$ are divisible by 5.
- A number is divisible by 10 if and only if its last digit is 0.

  Example. $40, 970, 13.375.910$ are divisible by 10.

Although it is quite easy to describe and understand the divisibility rules for some numbers, or deduce them from other number's divisibility rules, there are way many numbers whose divisibility rules aren't as easy and require much more complicated calculation.

Example. A number divisible by 6 if and only if it is divisible by 2 and by 3.
To know if a number is divisible by 13, we have to do some calculations: Let's suppose we want to know if the number $a_n a_{n-1} ... a_0$ where a_i is the i^{th} digit of the number is divisible by 13. This number is divisible by 13 if and only if $a_n a_{n-1} ... a_1 + 4 \times a_0$ is divisible by 13. Then we repeat this transformation until we obtain a number in the range from 1 to 52 $(= 13 \times 4)$. The number $a_n a_{n-1} ... a_0$ is divisible by 13 if and only if the result after the calculation is $13, 26, 39$. For example: $142.389 :\ 14.238 + 4 \times 9 = 14.274$, $1.427 + 4 \times 4 = 1.443$, $144 + 4 \times 3 = 156$, $15 + 4 \times 6 = 39$. Thus 142.389 is divisible by 13. Actually, it is possible to perform the division by 13 and check whether the remainder is 0. However the above criterion for 13 will be a special case of divisibility criteria that become very understandable when working with divisibility graphs, that are the objects of this work.

2 Divisibility

2.1 Notation

Notation. If x, y are integers, then we write $x \mid y$ (respectively, $x \nmid y$) if x divides (respectively, does not divide) y.

Definition. We say that "x is congruent to y modulo n" or "x and y are congruent modulo n" if and only if x and y have the same remainder in the euclidean division by n.

Notation. We write:

$$x \equiv y \mod n$$

Remark. In general, we have $0 < y < n$ such that y is the remainder of the euclidean division of x by n.

2.2 Testing divisibility in base b

Fix some natural number $b \geq 2$. Writing a positive integer number a in the numeral base b amounts to writing $a = \sum_{i=0}^{k} c_i b^i$ where $c_i \in \{0, 1, \dots, b-1\}$ are the digits in base b and the first digit c_k is non-zero. We want to test whether some integer $n \geq 2$ divides a:

- If $b \equiv 0 \bmod n$, we may replace a by c_0 (as a and its last digit leave the same remainder after division by n).
- If $b \equiv 1 \bmod n$, we may replace a by the sum of its digits in base b, namely $\sum_{i=0}^{k} c_i$ (as a and the sum of its digits leave the same remainder after division by n).
- If $b \equiv -1 \bmod n$, we may similarly replace a by the alternating sum of its digits in base b, namely $\sum_{i=0}^{k} c_i (-1)^i$.
- If $b \equiv 0 \bmod n$, calling β the remainder of b after division by n (thus $\beta \neq 0$), then we may replace a by $\sum_{i=0}^{k} \gamma_i \beta^i$.

Moreover, to test whether n divides a, we could suppose that n is a prime power. Indeed, if $n = \prod_{\ell \mid n} \ell^{v_\ell(n)}$ is the prime decomposition of n, then we may equivalently require that $\ell^{v_\ell(n)}$ divides a for all prime divisors ℓ of n.

3 Graph's Theory

3.1 Terminology

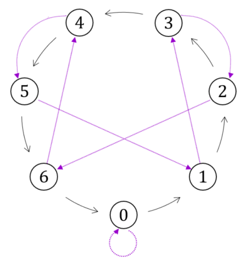
- **Order of a Graph** : the order of a graph is the number of vertices in the graph
- **Oriented Chain** : an oriented chain is a finite sequence of vertices linked together by oriented edges
- **Eulerian Chain** : an Eulerian chain is a simple oriented chain passing through all the edges of a graph
- **Cycle** : a cycle is a chain that returns to its starting point
- **Eulerian Cycle** : an Eulerian cycle is a simple cycle passing through all the edges of a graph only once
- **Connected Graph** : a graph is connected if for any pair of vertices (x,y), there is an oriented chain with first term x and last term y

3.2 Definitions

Definition. Graphs can be classified amongst to categories : oriented graphs, where the edges have no orientations and non-oriented graphs, where the edges are oriented by arrows. Both kinds of graphs have degrees, which are computed in two different ways. Degrees represent the number of edges connecting a vertex.

Definition. In an oriented graph, we also distinguish **indegrees** from **outdegrees**. The indegree of a vertex, denoted by $d^-(V_i)$, is the number of edges that go toward this vertex, whilst the outdegree, denoted as $d^+(V_i)$, is the number of edges that leave the vertex. In an oriented graph, the set of all the incoming edges is denoted by E_v^+ and the set of all the outgoing edges is denoted by E_v^-.

Example. Divisibility graphs will be in particular oriented graphs, here is an example:



Divisibility graph of 7

3.3 General properties of graphs

Here are some properties that come with the definitions seen above about both types of graphs.

For a non-oriented graph G with $|E|$ edges and $|V|$ vertices,

$$\sum_{i=1}^{k} d(V_i) = 2|E|$$

which means that the sum of the degrees of the vertices of a graph is equal to twice the number of edges of this graph.

For an oriented graph with $|E|$ edges and $|V|$ vertices, we have

$$\sum_{i=1}^{k} d^+(V_i) = |E| = d^-(V_i)$$

Corollary. *In a non-oriented graph, the number of vertices with odd degrees is even.*

Corollary. *In a non-oriented graph,* $d(V_i) = k \Rightarrow k|V| = 2|E|$

Corollary. *In a non-oriented graph,* $d(V_i) \geq k \Rightarrow k|V| \leq 2|E|$.

Corollary. *In a non-oriented graph,* $d(V_i) \leq k \Rightarrow k|V| \geq 2|E|$.

,

4 Divisibility Graphs

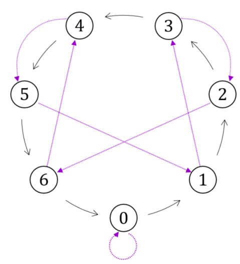
4.1 Divisibility graph's principle

We now define divisibility graphs which will be useful to understand divisibility criteria with reference to any positive integer n in basis 10 but also in any numeral basis $b \geq 2$.

Definition. The divisibility graph of n in basis b, which we denote by $D_{b,n} = (X_n, A_n)$ is an oriented graph, with $X_n = \{0, 1, ..., n-1\}$ the vertices and A_n the arrows.
We can define the arrows A_n as the union of the multiplicative and the additive arrows. The additive arrows $A_n^{(+)} = \{(i, j) \in D_{b,n} \mid j = i+1\}$ represent the operation $+1 \mod n$ and the multiplicative arrows $A_n^{(\times)} = \{(i, j) \in D_{b,n} \mid b \times i \equiv j \mod n\}$ represent the operation $\times b \mod n$.
From now on we consider the basis to be $b = 10$.

4.1.1 An example: the divisibility graph of 7

First let's look at the graph of 7 to understand the general principle:



Divisibility graph of 7

Two types of arrows can be recognised in the divisibility graph of 7. The black arrows $A_n^{(+)}$, representing the operation: $+1 \mod 7$, and the purple arrows $A_n^{(\times)}$, representing the operation: $\times 10 \mod 7$.

How does it work?

Let's suppose we want to determine whether a number $a = a_n a_{n-1} ... a_0$ where a_i is the i^{th} digit of a is divisible by 7 or not. We first start our walk at the vertex 0 and move a_n black arrows forward to another vertex, from which we take the one purple outgoing arrow, which will bring us to a next vertex. We repeat this process for a_{n-1} then a_{n-2}, etc... until a_1. Finally for a_0, we simply follow a_0 black arrows. If we land on the vertex 0, a is divisible by 7, otherwise it's not.

Why does it work?

Simply because every number can be decomposed as:

$$a = \sum_{i=0}^{n} a_i (10)^i$$

4.1.2 Generalisation: the divisibility graph of k

Recall that every positive integer $a = a_n a_{n-1} ... a_0$ where a_i is the i^{th} digit of a in base 10, and where $a_n \neq 0$. As every number a can be decomposed as

$$a = \sum_{i=0}^{n} a_i (10)^i$$

where a_i is the i^{th} digit of a. We repeat the following algorithm:

- Fix $r_1 =$ remainder of Euclid's division of a_n by k
- While $1 \leq i < n$, do
  1. Fix $r_2 =$ remainder of Euclid's division of $r_1 \times 10 \mod k$ by k
  2. Fix $r_1 =$ remainder of Euclid's division of $r_2 + a_{n-1}$ by k
  3. Fix $i = i - 1$
- $r_0 =$ Euclid's division of $a_1 + a_0$ by k

If $r_0 = 0$ then a if divisible by k, if r_0 is different from 0, then a is not divisible by 0.

4.2 Testing divisibility with a walk on a divisibility graph

Write a non-negative integer $a = \sum_{i=0}^{k} a_i b^i$ in base b. To test whether n divides a for some integer $n \geq 2$, consider the following walk on the divisibility graph $D_{b,n}$. Start from the vertex 0, and take a_k times an additive edge $A_n^{(+)}$. If $k > 0$, then for $i = 0, 1, \dots, k-1$ do the following: take the outgoing multiplicative edge $A_n^{(\times)}$ from the vertex on which you have landed, then walk a_i times on an additive edge. We have divisibility if and only if this walk ends at the vertex 0. The proof of the validity of the divisibility test amounts to considering the modulo n version of the following statement:

Lemma. *Any non-negative integer a can be obtained from* 0 *(in a unique way) by alternating the following two operations: adding some number from* 0 *to* $b-1$*; multiplying by b. The numbers to be added are precisely the digits of a in base b, from left to right.*

Proof. This is clear for the numbers up to $b-1$, with only one digit in base b. If $a \geq b$, then divide a by b, with quotient $q > 0$ and remainder r. Since $a = bq + r$, the last operations to be done are multiplying q by b and adding r. We conclude by induction, as q has one digit less than a. □

4.3 Edges of divisibility graphs

Some multiplicative edges of $D_{b,n}$ could be a loop, the reverse of an additive edge, or an additive edge. More precisely, we have:

Proposition. *Let $n, b \in \mathbb{N}$, the divisibility graph $D_{b,n}$ has the following property:*

$$(a,a) \in A_n^{(\times)} \Leftrightarrow a \equiv ba \mod n$$

Proof. This means that $n \mid a(b-1)$ or in other words, a is a multiple of $n/\gcd(n, b-1)$. So we always have a loop at 0, and this is the only loop if $b-1$ is a unit. The number of loops is always equal to $gcd(b-1,n)$. $\square$

Proposition. *We similarly have:*

$$(a,a) \in A_n^{(+)} \Leftrightarrow a+1 \equiv ba \mod n$$

Proof. The congruence in the statement is equivalent to $a(b-1) \equiv 1 \bmod n$. This happens if and only if $b-1$ is a unit modulo n and a is its inverse. Similarly, a multiplicative edge is the reverse of an additive edge if and only if $a-1 \equiv ba \bmod n$, i.e. $b-1$ is a unit and $-a$ is its inverse. $\square$

Proposition. *With the above notation, we have*

$$\#A_n^{(\times)} = \begin{cases} 2n & \textit{if} \quad b-1 \quad \textit{is a zero divisor} \\ 2n-1 & \textit{if} \quad b-1 \quad \textit{is a unit} \end{cases}$$

as we do not count the multiplicative edges that are additive edges.

Proof. If $b-1$ is a zero divisor, then the number of edges exiting the n-gon (excluding the loops, the additive edges and their reverses) is $n-3$. If $b-1$ is a unit, then $b-1$ and n are coprime, hence their gcd $isequaltooneandthenumberofloopsinthegraphwillbeequaltoone,andwillbelocatedatthev$ In some cases it could be convenient to count edges with multiplicities, namely to assign multiplicity 2 to an edge which is an additive edge and a multiplicative edge.

4.4 Adjacency Matrix

Definition. Let $G = (X_n, A_n)$ be an oriented graph, with $X_n = \{0, 1, ..., n-1\}$ and A_n the set of oriented matrix. The adjacency matrix of the graph G is the matrix $M(G) \in$

$\mathrm{Mat}_{n\times n}(\mathbb{R})$ whose coefficient $m_{i,j}$ are defined by the following rule:

$$m_{i,j} = \begin{cases} 1 & \text{if} \quad (x_i, x_j) \in A \\ 0 & \text{if} \quad (x_i, x_j) \notin A \end{cases}$$

Proposition. *We have that for each* $i = \{1, 2, ..., n\}$*,*

$$d^+(i) = \sum_{j=1}^{n} m_{i,j}$$

$$d^-(i) = \sum_{j=1}^{n} m_{j,i}$$

$$\sum_{m_{i,j}} = \sum_{i=1}^{n} d^+(i) + \sum_{i=1}^{n} d^-(i) = |A|$$

where $d^+(i)$ *is the number of arrows of initial vertices i (going from i), and* $d^-(i)$ *is the number of arrows of final vertices i (coming to i).*
Moreover the trace of the matrix $M(G)$ *is equal to the number of loops in the graph*

Remark. For non oriented graphs, the adjacency matrix is symmetric.

Remark. For a divisibility graph, there is the possibility that two arrows (one multiplicative and one additive) go from the vertices i to the vertices j (for example in the graph of 7, two arrows go from 4 to 5), thus, to calculate the degree of each vertex, we have to write the number of arrows for each $m_{i,j}$. In other words:

$$m_{i,j} = 2 \Leftrightarrow (i, j) \in A_n^{(\times)} \cap A_n^{(+)}$$

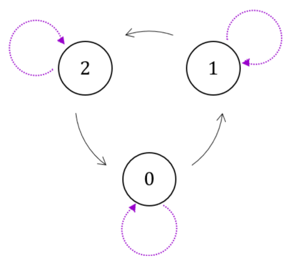
Theorem. *Let* $G = (X, A)$ *be an oriented graph, with* $X = \{x_1, x_2, ..., x_n\}$*, and consider its adjacency matrix* $M = (m_{i,j})$*. For all positive integer k, we write* $M^k = (m_{i,j}^{(k)})$*. Then* $(m_{i,j}^{(k)})$ *is equal to the number of paths of length k from the vertex* x_i *to the vertex* x_j*.*

Proof. Eric Sigward, Introduction à la théorie des graphes, Académie Nancy-Metz, Mars 2002 □

4.5 Examples of divisibility graphs

Here are some examples of divisibility graphs with their adjacency matrix.

1. The divisibility graph of 3



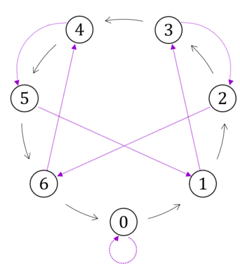
Divisibility graph of 3

and its adjacency matrix

$$M_3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

We can see that $Tr(M_3) = 3$ so that represents the 3 loops of the graph and for all $i = \{1,2,3\}$ we have that $\quad d^+(x_i) = 2, \quad d^-(x_i) = 2$, d^- being the outgoing degree and d^+ the ingoing degree.

2. The divisibility graph of 7

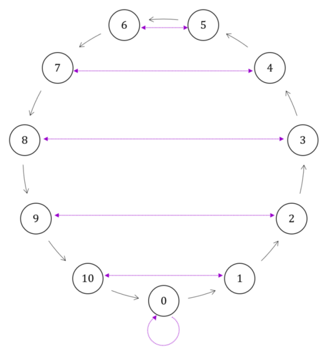


Divisibility graph of 7

and its adjacency matrix

$$M_7 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

3. The divisibility graph of 11

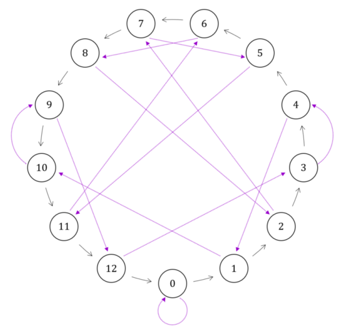


Divisibility graph of 11

and its adjacency matrix

$$M_{11} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

4. The divisibility graph of 13



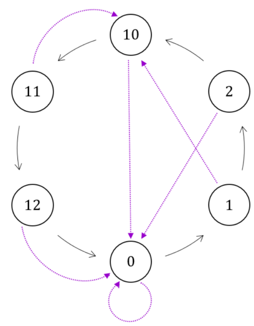
Divisibility graph of 13

and its adjacency matrix

$$M_{13} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

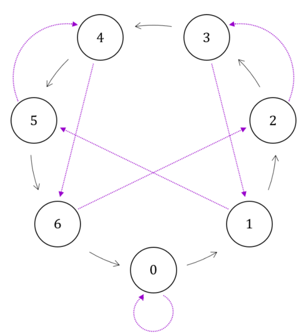
Now let's look at the divisibility graph in another base:

- $D_{3,6}$



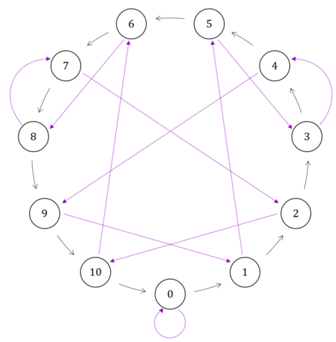
Divisibility graph of 6 in base 3

- $D_{5,7}$



Divisibility graph of 7 in base 5

- $D_{5,11}$

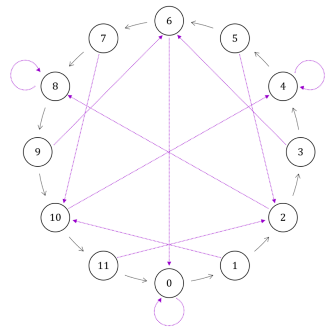


Divisibility graph of 11 in base 5

Remark. When b divides n, then it is possible to draw a divisibility graph while writing all the vertices in base b : for example the graph $D_{3,6}$.
However for other numbers it is not possible : for example the graph of 7 in base 5: $(7)_{10} = (12)_5$ and $(5)_{10} = (10)_5$, then the remainder of the euclidean division of 2×10 by 12 is equal to 8 which is not a digit in base 5. Thus if we want to draw the divisibility graph of n in base b with $b \nmid n$ we keep the number in base 10 and we calculate the rest of the euclidean division of $k \times b$ ($k \in \mathbb{N} | k < n$ by n to draw the multiplicative arrows. But to verify if a number is divisible by n, we have to use its form in base b.

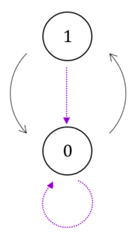
4.6 Quotient Graphs

While computing different graphs, we noticed that for the graph of a non prime integer, we could see the pattern of the graphs of its divisors. Let's take the example of the divisibility graph of 12:

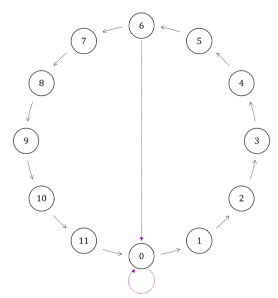


Divisibility graph of 12

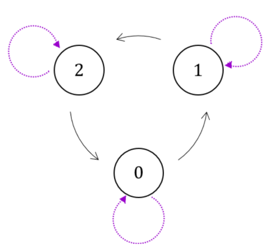
The divisors of 12 are $2, 3, 4$ and 6. Let's compare the graphs of the divisors of 12 with its divisibility graph.



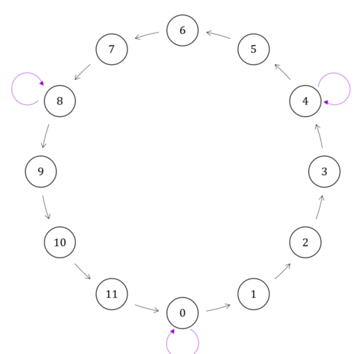
Divisibility graph of 2



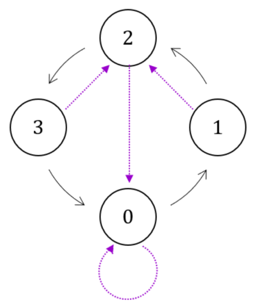
Pattern of the divisibility graph of 2 in the graph of 12



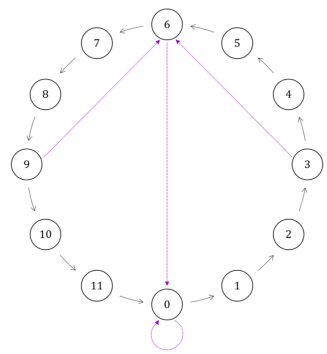
Divisibility graph of 3



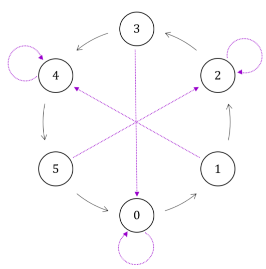
Pattern of the divisibility graph of 3 in the graph of 12



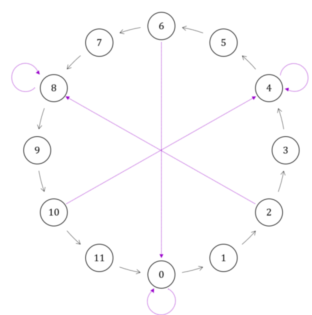
Divisibility graph of 4



Pattern of the divisibility graph of 4 in the graph of 12



Divisibility graph of 6



Pattern of the divisibility graph of 6 in the graph of 12

We will now try to formulate this idea in a more precise way.

Definition (Divisibility Quotient)**.** Let $D_n = (X_n, A_n)$ be the divisibility graph of n with X_n the set of vertices and A_n the set of edges and let

$$\begin{array}{rrcl} \phi : & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \\ & x \mod n & \mapsto & x \mod m \end{array}$$

be the natural projection. The homomorphism ϕ is surjective, thus for all , $ji \in \mathbb{Z}/m\mathbb{Z}$, there exits $a, b \in \mathbb{Z}/n\mathbb{Z}$ such that $\phi(a) = i$ and $\phi(b) = j$.

We obtain the graph D_ϕ as follows:

$$X_\phi = \{0,1,\dots,m-1\}$$
$$(i,j) \in A_\phi \quad \text{if} \quad (a,b) \in A_n$$

Remark. In this case: $\forall k \in \mathbb{Z}/n\mathbb{Z}$, we have: $\phi(k) = \overline{k}_m$
With $k \equiv \overline{k}_m \mod m$.

Theorem. *Assume $d|n$. Then the graph D_d is a quotient of the graph D_n. Moreover, if $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ denotes the natural projection, we have $D_\phi \cong D_d$.*

Proof. Assume $d|n$, and let's define the function $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}, x \mapsto \bar{x}$, where $\bar{x}$ is the class of x.
We identify the vertices accordingly.
Now to identify the edges: suppose there is an arrow from the vertex x to the vertex y, denoted by $x \sim y$ in the graph D_n. It means that $10x \equiv y \mod n$. This implies, working with the class of x and y denoted respectively $\bar{x}$ and $\bar{y}$, that $10\bar{x} \equiv \bar{y} \mod d$, so that there exists the edge $\bar{x} \sim \bar{y}$ in the graph D_ϕ.
But the graph of D_ϕ is isomorphic to the graph of D_d, thus the graph $D_\phi = (X_\phi, A_\phi)$ is equal to the graph $D_d = (X_d, A_d)$.
To conclude: $\forall x \sim y \in D_n \Rightarrow \bar{x} \sim \bar{y} \in D_d = (X_d, A_d)$. $\square$

Example. Let's take the example of the divisibility graph of 12:

1. We identify first the vertices:

   - Let's take the divisor 6:
     $$\begin{array}{rccr} \phi_6 : & \mathbb{Z}/12\mathbb{Z} & \longrightarrow & \mathbb{Z}/6\mathbb{Z} \\ & 0,6 & \longmapsto & 0 \\ & 1,7 & \longmapsto & 1 \\ & 2,8 & \longmapsto & 2 \\ & 3,9 & \longmapsto & 3 \\ & 4,10 & \longmapsto & 4 \\ & 5,11 & \longmapsto & 5 \end{array}$$
   - Let's take the divisor 4:
     $$\begin{array}{rccr} \phi_4 : & \mathbb{Z}/12\mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \\ & 0,4,8 & \longmapsto & 0 \\ & 1,5,9 & \longmapsto & 1 \\ & 2,6,10 & \longmapsto & 2 \\ & 3,7,11 & \longmapsto & 3 \end{array}$$

- Let's take the divisor 3:

$$\begin{array}{llcr} \phi_3: & \mathbb{Z}/12\mathbb{Z} & \longrightarrow & \mathbb{Z}/3\mathbb{Z} \\ & 0,3,6,9 & \longmapsto & 0 \\ & 1,4,7,10 & \longmapsto & 1 \\ & 2,5,8,11 & \longmapsto & 2 \end{array}$$

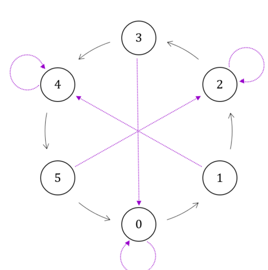
- Let's take the divisor 2:

$$\begin{array}{llcr} \phi_2: & \mathbb{Z}/12\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & 0,2,4,6,8,10 & \longmapsto & 0 \\ & 1,3,5,7,9,11 & \longmapsto & 1 \end{array}$$

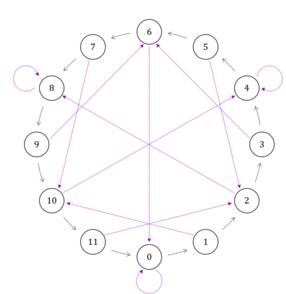
2. Now we identify each edge (let's do it for the graph of 6):

$$\begin{array}{ccccccccl} x & \sim & y & \Rightarrow & \overline{x} & \sim & \overline{y} & ; & 10\times x \equiv y' \mod 6 \\ 0 & \sim & 0 & \Rightarrow & 0 & \sim & 0 & ; & 10\times 0 \equiv 0 \mod 6 \\ 1 & \sim & 10 & \Rightarrow & 1 & \sim & 4 & ; & 10\times 1 \equiv 4 \mod 6 \\ 2 & \sim & 8 & \Rightarrow & 2 & \sim & 2 & ; & 10\times 2 \equiv 2 \mod 6 \\ 3 & \sim & 6 & \Rightarrow & 3 & \sim & 0 & ; & 10\times 3 \equiv 0 \mod 6 \\ 4 & \sim & 4 & \Rightarrow & 4 & \sim & 4 & ; & 10\times 4 \equiv 2 \mod 6 \\ 5 & \sim & 2 & \Rightarrow & 5 & \sim & 2 & ; & 10\times 5 \equiv 4 \mod 6 \\ 6 & \sim & 0 & \Rightarrow & 0 & \sim & 0 & ; & 10\times 0 \equiv 0 \mod 6 \\ 7 & \sim & 10 & \Rightarrow & 1 & \sim & 4 & ; & 10\times 1 \equiv 4 \mod 6 \\ 8 & \sim & 8 & \Rightarrow & 2 & \sim & 2 & ; & 10\times 2 \equiv 2 \mod 6 \\ 9 & \sim & 6 & \Rightarrow & 3 & \sim & 0 & ; & 10\times 3 \equiv 0 \mod 6 \\ 10 & \sim & 4 & \Rightarrow & 4 & \sim & 2 & ; & 10\times 4 \equiv 2 \mod 6 \\ 11 & \sim & 2 & \Rightarrow & 5 & \sim & 4 & ; & 10\times 5 \equiv 4 \mod 6 \end{array}$$

It is clear that $y = y'$ so that the identification of each edge corresponds to the edge of the graph D_6.

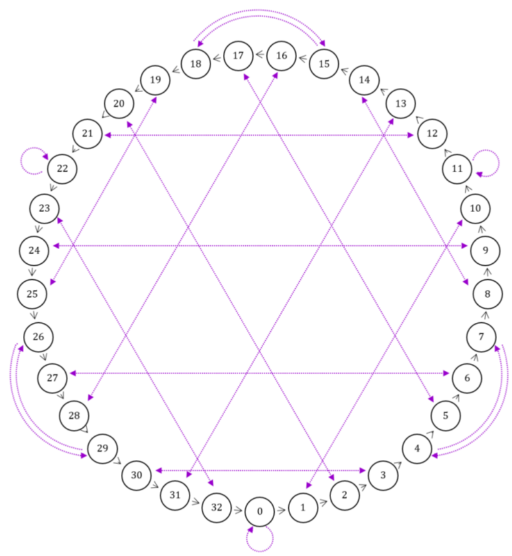


Divisibility graph of 6



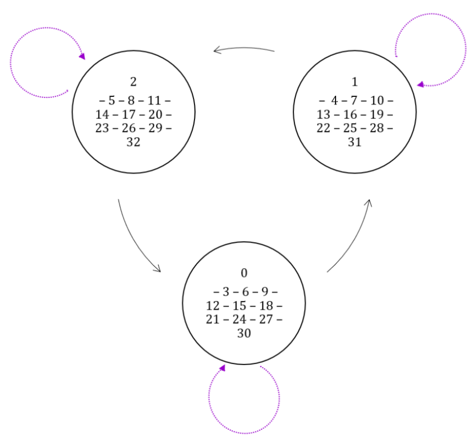
Divisibility graph of 12

Now let's take the example of the graph of 33:

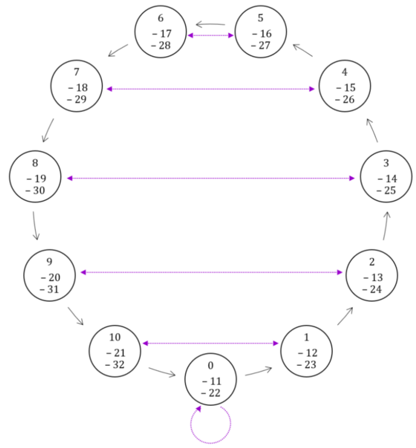


Divisibility graph of 33

The divisors of 33 are 3 and 11.



Quotient divisibility graph of 33 by 3

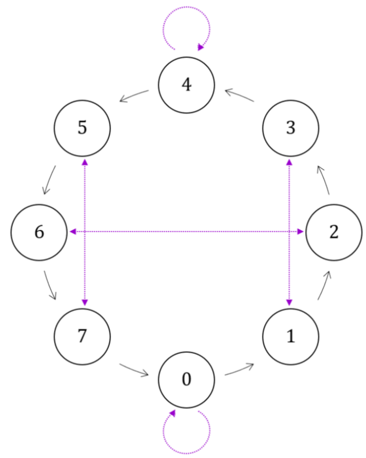


Quotient divisibility graph of 33 by 11

4.7 On the Eulerianity of divisibility graphs

An oriented graph is *Eulerian* if and only if at each vertex there is the same amount of oncoming and incoming edges. At each vertex there is one incoming and one oncoming additive edge.

If b is a unit, then there is one incoming and one outcoming multiplicative edge at each vertex (they may coincide, e.g. consider the loop at 4 in $D_{3,8}$): if we count edges with multiplicity, then $D_{b,n}$ is Eulerian; if $b-1$ is a unit and we do not count multiplicative edges that are additive edges, then $D_{b,n}$ is not Eulerian, as the inverse of $b-1$ has 1 oncoming edge and 2 incoming edges. If b is not a unit, then $D_{b,n}$ is not Eulerian because there is no incoming multiplicative edge at vertices that are units (if we do not count multiplicative edges that are additive edges, then we need $n > 2$ because we cannot work with the inverse of $b-1$).

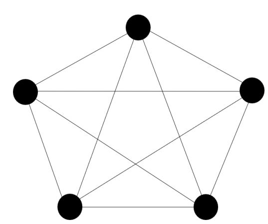


$D_{(3),8}$

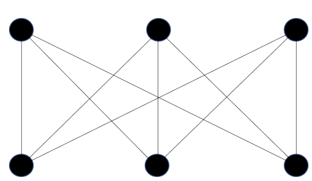
4.8 On the planarity of divisibility graphs

Roughly speaking, a graph is *planar* if it can be drawn in the plane so that the edges do not intersect (we can ignore the orientation of the edges). By the well-known Wagner's theorem,

Theorem. *A finite graph is planar if and only if it does not contain a copy of K_5 nor of $K_{3,3}$, which are the two graphs below:*

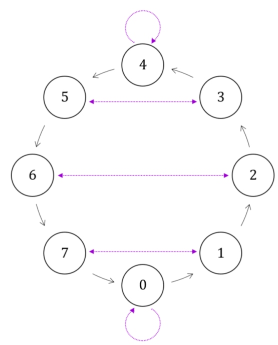


Graph of K_5



Graph of $K_{3,3}$

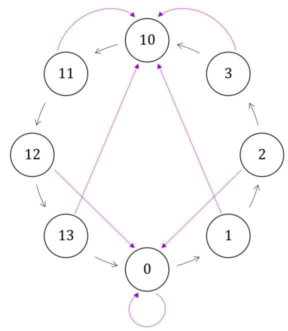
For example, $D_{4,6}$ contains a copy of $K_{3,3}$ while $D_{6,15}$ contains a copy of K_5 so they are not planar. The graphs $D_{0,n}$, $D_{1,n}$, $D_{n-1,n}$ are planar. The multiplicative edges of $D_{0,n}$ all go to zero, so they can be drawn as diagonals of the regular n-gon, while the multiplicative edges of $D_{1,n}$ are loops. The graph $D_{n-1,n}$ is planar because the multiplicative edges can be drawn very closely to diagonals of the regular n-gon that are orthogonal to the line connecting 0 and the center of the n-gon. Example of a graph $D_{n-1,n}$: $D_{7,8}$



Divisibility graph of 8 in base 7

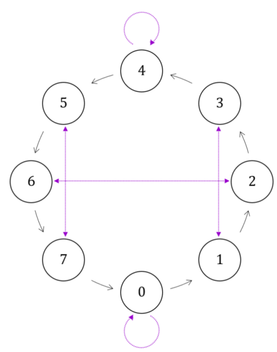
If n is even, the graphs $D_{n/2,n}$ and $D_{n/2-1,n}$ are planar. For $D_{n/2,n}$, the multiplicative edges go to 0 or to $n/2$: the former can be drawn as diagonals of the regular n-gon, while the latter can be drawn outside of the polygon. For $D_{n/2-1,n}$ the multiplicative edges connecting vertices v and $-v$ can be drawn as non-intersecting diagonals of the regular n-gon, while those connecting vertices v and $n/2-v$ can be drawn as circular arcs outside of the polygon: these do not intersect as we can take smaller arcs for v going from 0 to $n/4$ or $n/4+1$ respectively.

- Example of a graph $D_{n/2,n}$: $D_{4,8}$



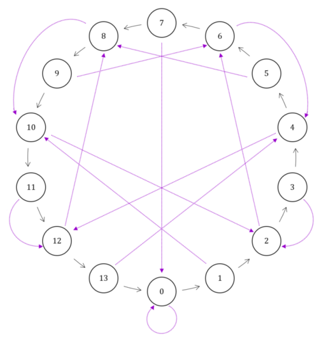
Divisibility graph of 8 in base 4

- Example of a graph $D_{n/2-1,n}$: $D_{3,8}$



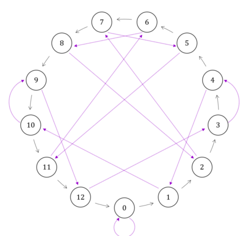
Divisibility graph of 8 in base 3

Conjecture (Wolff)**.** Suppose $b \neq 0, 1, n-1, n/2, n/2-1$. The divisibility graph $D_{b,n}$ is not planar if $n \geq 13$ is odd, or if $n \geq 16$ is even.

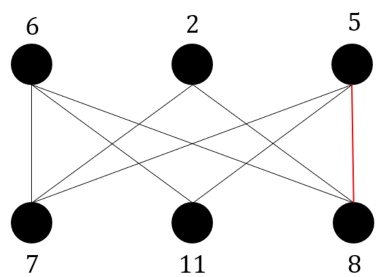


Divisibility graph of 14 in base 10

This graph is planar so it agrees with the conjecture of Wolff. Let's take a look at a graph that is non planar according to the conjecture: for example the graph of 13. Then, we should be able to find the graph K_5 or $K_{3,3}$ in it.

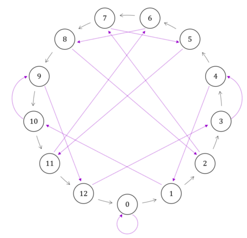


Divisibility graph of 13

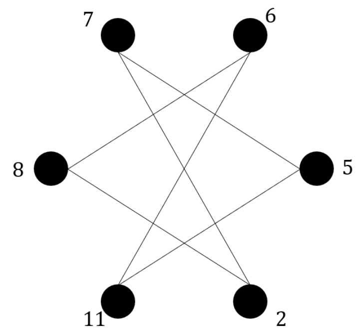


$K_{3,3}$ applied to the divisibility graph of 13

We can see that the edge $(5,8)$ does not exists thus it is impossible for the graph $K_{3,3}$ to be a sub-graph of 13.

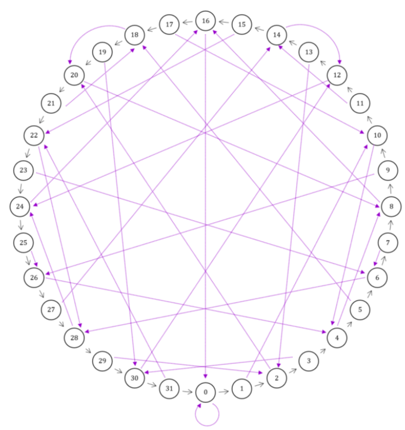


Divisibility graph of 13



K_5 applied to the divisibility graph of 13

Here we can see that the "star" has six points instead of 5. So K_5 isn't a sub-graph of D_{13}.



Divisibility graph of 32 in base 10

This graph is supposed to be non-planar according to the conjecture of Vincent Wolff, but the graphs K_5 or $K_{3,3}$ don't seem to appear in it, which would suggest that the conjecture has to be slightly modified, since non-planar graph are supposed to contain K_5 or $K_{3,3}$. Notice that the conjecture does not concern the graph $D_{10,14}$, which is planar and indeed does not contain neither K_5 nor $K_{3,3}$.

5 More on the Graph's Theory

5.1 Symmetries

Consider the graph $D_{b,n}$ as not oriented, and draw it as a geometric figure, recalling that we place the vertices at a regular n-gon. More precisely, the edges that are not loops are segments connecting vertices, while the loops are small circles around the vertices. Then we may ask whether $D_{b,n}$ is symmetric at the line L_z through a vertex z and the center of the regular n-gon. Such a symmetry swaps the vertices x and $2z-x$. For example, if n is even and $z=n/2$, then it swaps x and $n-x$: as we will see below, $D_{b,n}$ is symmetric at $L_{n/2}$.

There is no problem is swapping additive edges. The symmetry condition for the loops is that $n \mid a(b-1)$ implies $n \mid (2z-a)(b-1)$ for every a or, in other words, that $n \mid 2z(b-1)$. Finally, we have to ensure that multiplicative edges connecting non-consecutive vertices are also symmetric. Supposing that $ba \neq a, a+1, a-1$, the condition for a is that $b(2z-a) = 2z-ba$ or $b(2z-ba) = 2z-a$. This means $n \mid (b-1)2z$ or $n \mid (b-1)(2z-a(b+1))$.

Definition (Weak symmetry)**.** We define the weak symmetry for a graph if there exists for each vertex $x \sim y$ a vertex $y \sim x$. But we do not count the loops.

Proposition. *Every divisibility graph of n in base $b = n-1$ has weak symmetry.*

Proof. We want to prove that for every arrows $(i,j) \in A_n^{(\times)}$, there exists an arrow $(j,i) \in A_n^{(\times)}$. First we have:

$$\begin{aligned} (i,j) \in A_n^{(\times)} \quad &\Leftrightarrow \quad (n-1)i \equiv j \mod n \\ &\Leftrightarrow \quad (n-1)i = kn + j \qquad\qquad k \in \mathbb{N} \end{aligned}$$

Thus we have

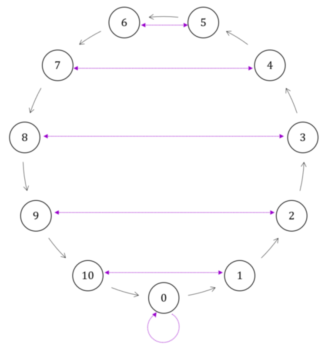
$$j = (n-1)i - kn$$

Now, we want to show that there is an arrow (j,i):

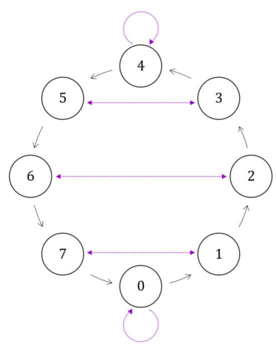
$$\begin{aligned} (n-1)j \quad &= \quad (n-1) \times [(n-1)i - kn] \\ &= \quad (n-1)^2 i - (n-1)kn \\ &= \quad n(ni - 2i - k + kn) + i \\ &= \quad pn + i \qquad\qquad\qquad\qquad p = ni - 2i - k + kn \in \mathbb{Z} \\ &\Rightarrow \quad (j,i) \in A_n^{(\times)} \end{aligned}$$

So the divisibility graph $D_{(n-1),n}$ has weak symmetry. $\square$

Example. Here are some examples:



Divisibility graph of 11 in base 10



Divisibility graph of 8 in base 7

5.2 Periodic points

Consider the multiplication by b on the vertices of $D_{b,n}$, and the iterates of this map. As the graph is finite, all vertices are pre-periodic points.

Call g_∞ the limit for $x \to \infty$ of the eventually constant sequence $\gcd(b^x, n)$ and set $n_\infty := n/g_\infty$. Then the *periodic points* are precisely the vertices v such that $\gcd(v,n)$ is a multiple of g_∞. Indeed, the periodic points are divisible by g_∞ because $\gcd(v,n)$ must be the same for all vertices v in the orbit of a periodic point. Moreover, the multiples of g_∞ are periodic points because they are the image of $\mathbb{Z}/n_\infty$ in $\mathbb{Z}/n$ and $(b \bmod n_\infty)$ is a unit modulo n_∞.

Thus 0 is the only periodic point if and only if $g_\infty = n$. Moreover, all points are periodic if and only if $g_\infty = 1$, i.e. b is a unit.

The size of the orbit of a periodic point a is the smallest positive integer x such that $n_\infty \mid a(b^x - 1)$ thus it divides the size of the orbit of g_∞. If b is a unit, the size of the orbit of 1 is precisely the smallest positive integer x such that $n \mid (b^x - 1)$: this order is maximal when it equals $\varphi(n)$, and in this case all units lie in one same orbit.

By fixing n and varying b, the possible values for g_∞ are 2^d, where d is the number of prime divisors of n because g_∞ can be obtained from n by removing all prime factors that do not divide b. We may then characterize 2^d as the different sets of periodic points in the graph $D_{b,n}$ by varying b.

6 Miscellanea

6.1 Criterion for n being a prime power

In a graph, we call *neighbour* of a vertex v any vertex which is related to v by an edge (the direction of the edge does not matter).

Theorem. *An integer $n \geq 2$ is a prime power if and only if for every $2 \leq b < n$ the divisibility graph $D_{b,n}$ has some vertex with at most two neighbours except possibly itself. In other words, we want some vertex v such that the multiplicative edges starting or ending at v are loops or additive edges or the reverse of additive edges.*

Proof. Notice that an integer $n \geq 2$ is a prime power if and only if for every integer $2 \leq b < n$ we have that b or $b-1$ is a unit (because, if n has two distinct prime divisors p and q, then the condition does not hold for example if $b \equiv 1 \bmod p$ and $b \equiv 0 \bmod q$). If b is a unit, we may take $v = 0$. If b is a zero divisor and $b-1$ is a unit, then we may take as v the inverse of $b-1$: the multiplicative edge starting at v is an additive edge; no multiplicative edge ends at v because b is a zero divisor and v is a unit.
Now suppose that b and $b-1$ are zero divisors, and in particular $\gcd(n,b) > 1$. If v is as requested, the multiplicative edge at v must be a loop (as no multiplicative edge is an additive edge or its reverse) thus $v \equiv bv \bmod n$. To conclude, we find some vertex $w \neq v$ such that the multiplicative edge at w ends at v, i.e. $v \equiv bw \bmod n$: we can take any $w \neq v$ such that $w \equiv v \bmod n/\gcd(n,b)$. □

6.2 Skeletons of Polyhedra

Consider a three-dimensional convex polyhedron and its *skeleton*, namely the graph where vertices and (not oriented) edges are those of the polyhedron. For example, the skeleton of a tetrahedron can be drawn in the plane as follows: draw the vertices of an equilateral triangle and its middle point; draw the 6 connecting segments between those 4 points.

Conjecture (Wolff)**.** No divisibility graph is the skeleton of a three-dimensional convex polyhedron.

A graph is 3-*connected* if it is connected and it is still connected by removing any two vertices (and all edges at them). By a well-known :

Theorem (Steinitz)**.** *A graph G is the edge graph of a polyhedron if and only if G is a simple planar graph which is 3-connected.*

Notice that, if b or $b-1$ are units, then $D_{b,n}$ is not 3-connected: if b is a unit, then the only multiplicative edge at 0 is a loop; if b is a zero divisor and $b-1$ is a unit, then the multiplicative edge at the inverse of $b-1$ is an additive edge and there is no multiplicative edge ending at it. For example, if n is even, the graph $D_{n/2,n}$ is not 3-connected (remove 0 and $n/2$).

7 References

- Eric Sigward, Introduction à la théorie des graphes, Académie Nancy-Metz, Mars 2002
- Steinitz's theorem, Wikipedia
- Yvan Monka, Graphes, Académie de Strasbourg, 2018
- Laurent Guillopé, Graphes, Université de Lille, Février 2012
- Théorie specctrale des graphes, Wikipedia
- Graph Theory, Wikipedia
- Adjacency Matrix, Wikipedia
- Arithmétique en base b, Institut Saint-laurent
- F. Busato, N. Bombieri, Graph algorithms on GPUs, in Advances in GPU Research and Practice, 2017
- Emma Jordan, Fränk Plein, Mélina Van Weverberg, Adrien Vandenschrick, Les graphes en un coup de pinceau, Université de Bruxelles, 2014