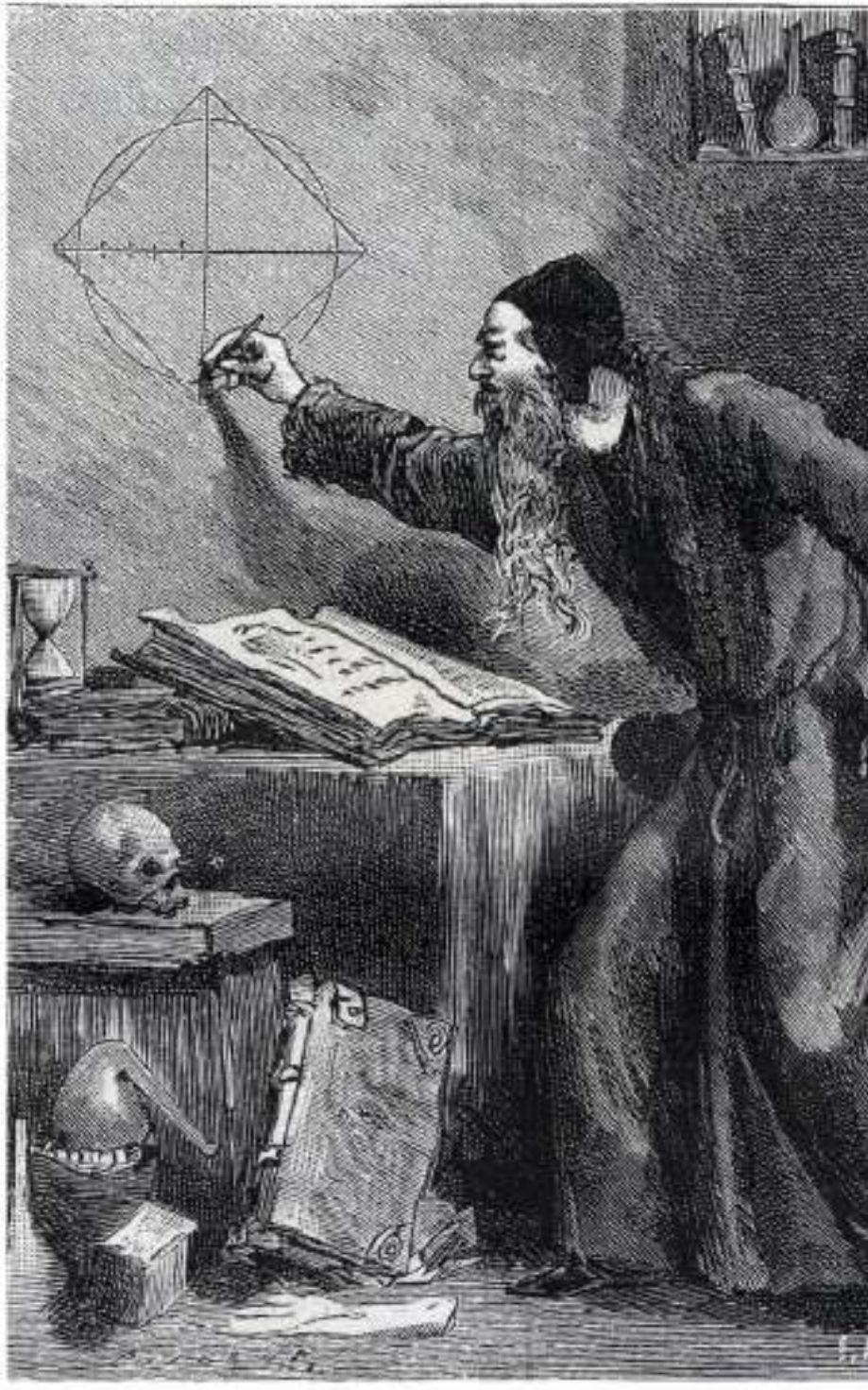
Les grands problèmes mathématiques de l'antiquité à nos jours

Frédéric HAVET

Institut Esope 21

TERRA NUMERICA



Principe Pythagoricien

Pour les Pythagoriciens, **"tout est nombre".**

Pythagore (-550 avant J.C.) a découvert les lois harmoniques : relation entre la longueur d'une corde vibrante et la hauteur du son émis.

Idée naturelle : toute longueur est commensurable à l'unité.
tout nombre peut s'exprimer comme une fraction.

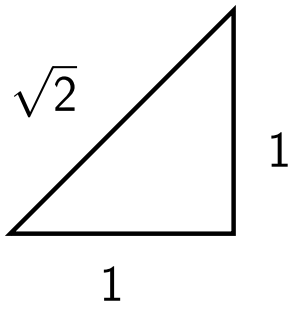
$\Longrightarrow$ à condition de bien choisir l'unité, on peut ne travailler que sur des figures dont les longueurs sont entières.

Malheureusement, c'est **FAUX**. $\sqrt{2}$ ne peut pas s'exprimer comme une fraction.

$\ll$ *There are proofs that date back to the Greeks that are still valid today* $\gg$

Andrew Wiles

Racine carrée de 2

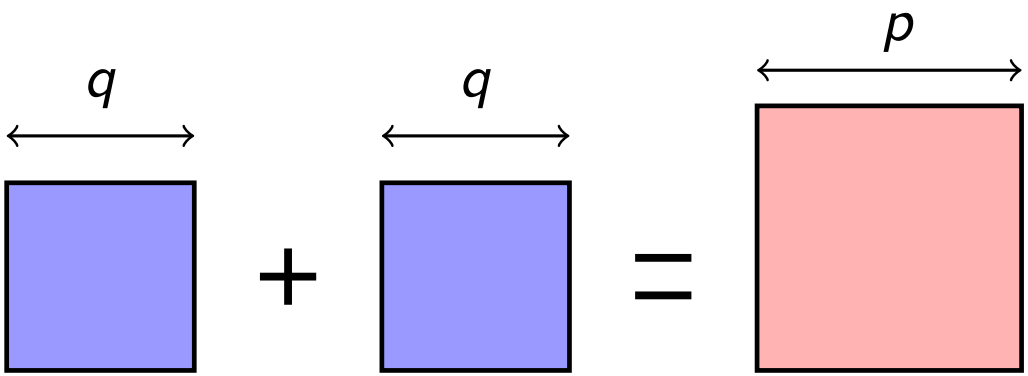


$\sqrt{2}$ est la longueur de la diagonale d'un carré de côté 1.

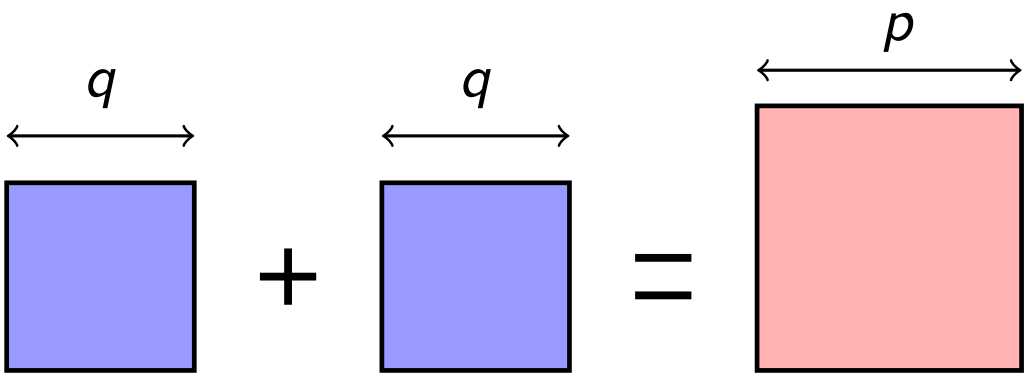
Pythagore : $\sqrt{2}^2 = 1^2 + 1^2 = 2$.

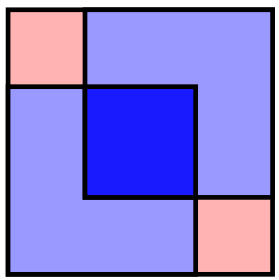
Supposons que $\sqrt{2} = \frac{p}{q}$.
$p = 2^i p_1$ et $q = 2^j q_1$ avec p_1 et q_1 impair.
$2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}$ soit $2q^2 = p^2$.
Ainsi $2 \times 2^{2j} q_1^2 = 2^{2i} p_1^2$. Donc $2j + 1 = 2i$, **impossible**.

Racine carrée de 2

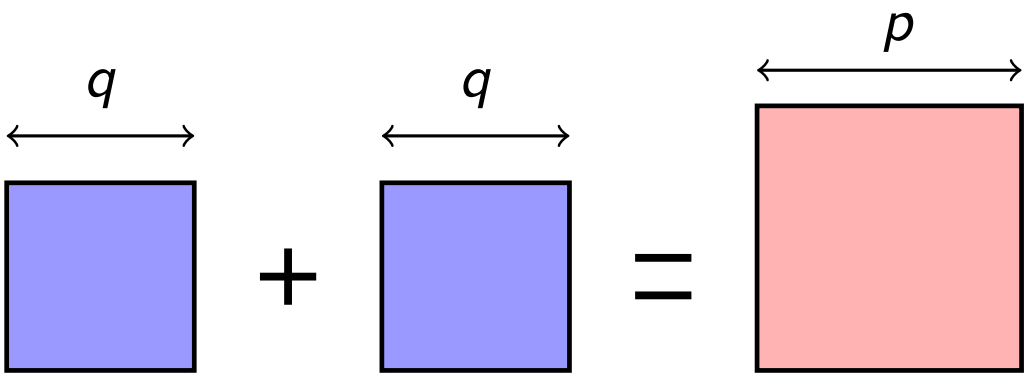


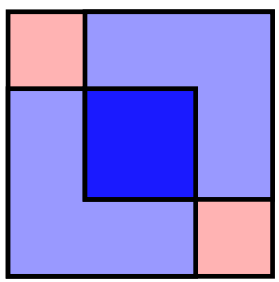
Racine carrée de 2

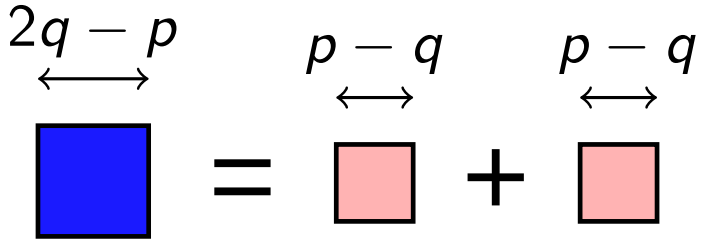




Racine carrée de 2







Nombres constructibles à la règle et au compas

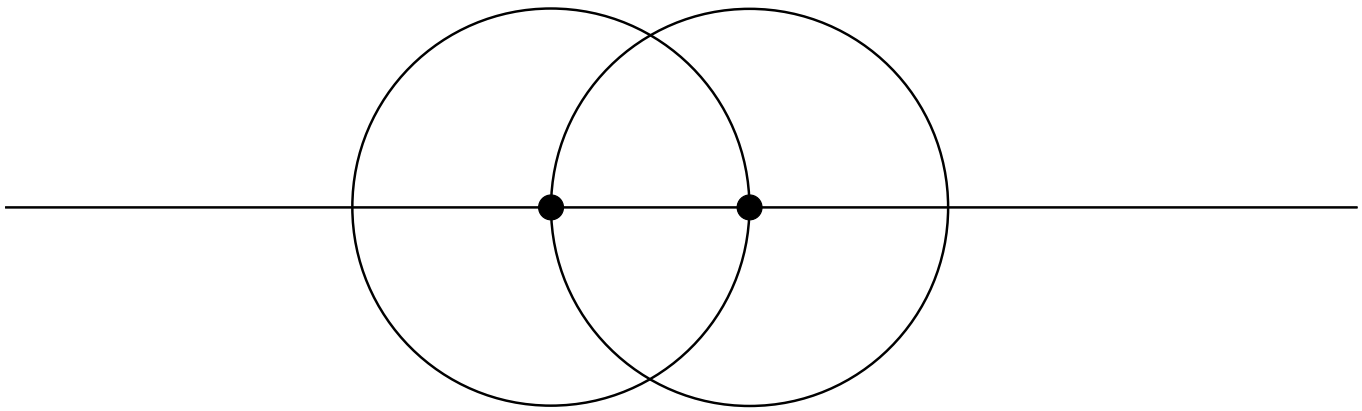
Les points, cercles et droites constructibles à la règle et au compas sont définis de la manière récursive suivante :

- (0,0) et (1,0) sont constructibles.
- Si deux points A et B sont constructibles alors la droite (AB) est constructible et le cercle de centre A et de rayon AB sont constructibles.
- L'intersection de deux cercles ou droites constructibles est constructibles.

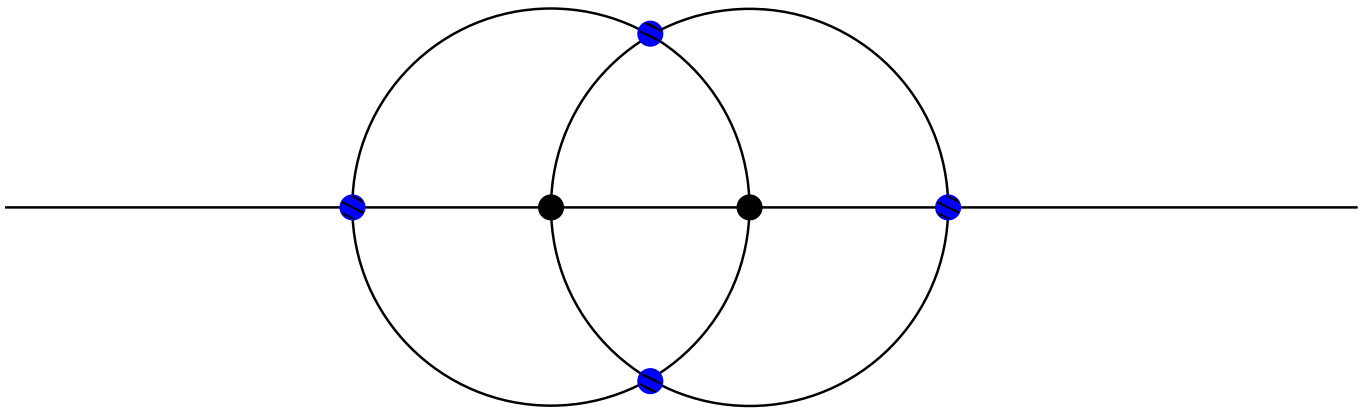
Un nombre constructible à la règle et au compas est la mesure d'une longueur associée à deux points constructibles à la règle (non graduée) et au compas.

Points constructibles en une étape

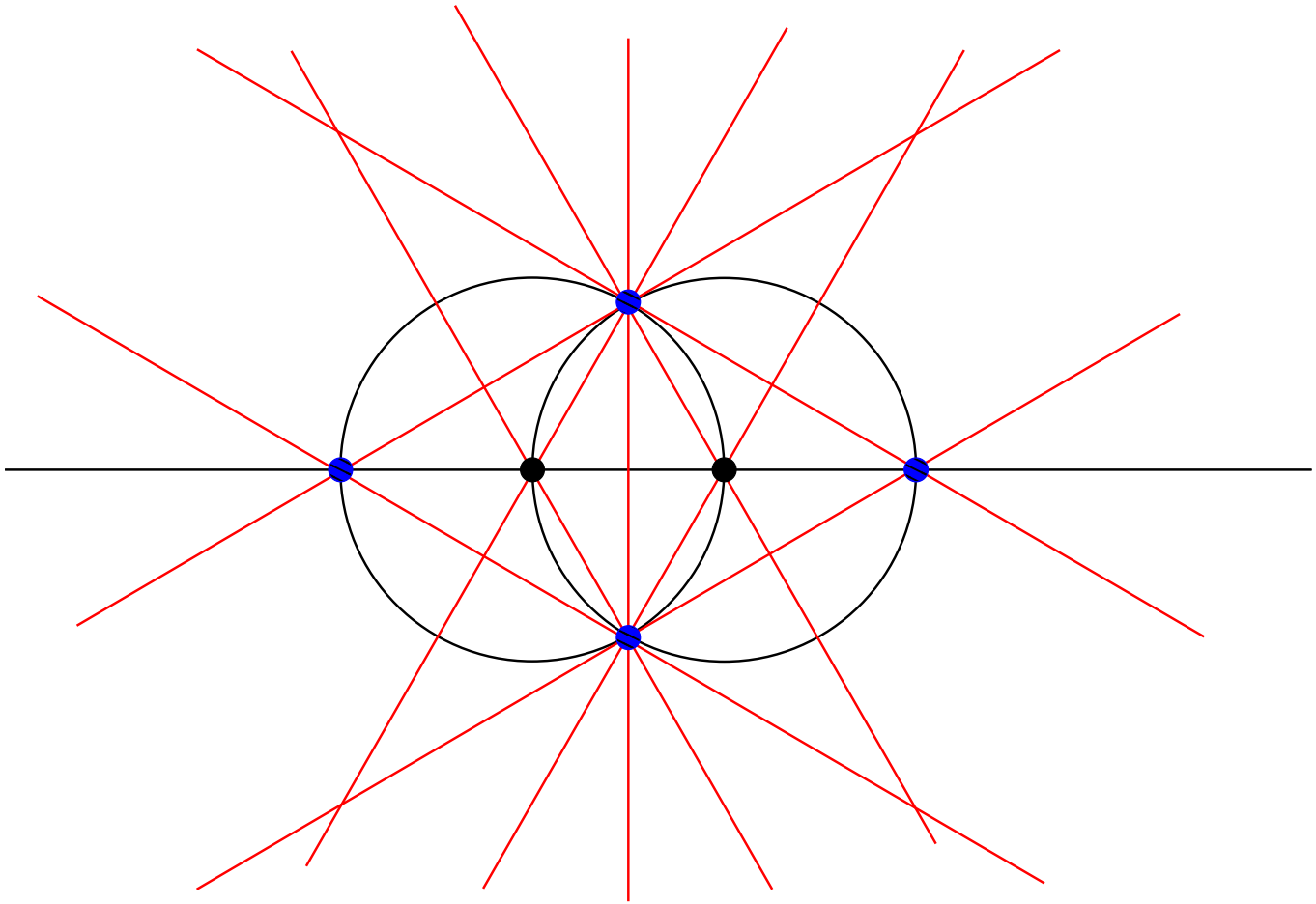
Points constructibles en une étape



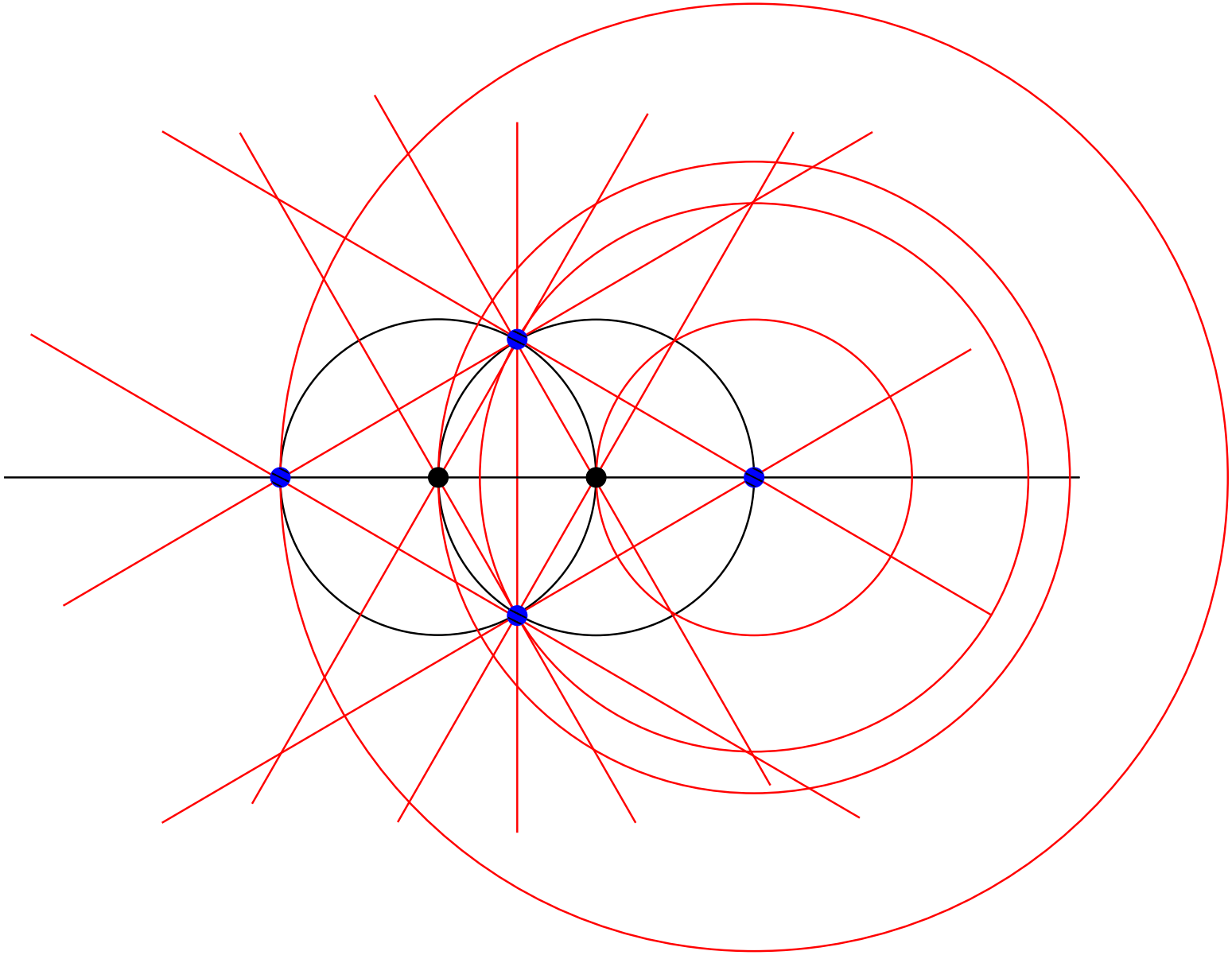
Points constructibles en une étape



Points constructibles en deux étapes



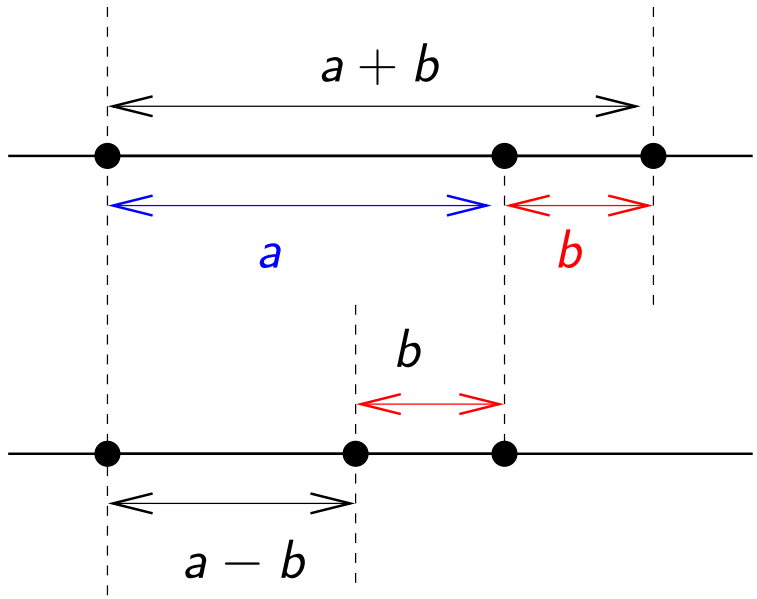
Points constructibles en deux étapes



Addition et soustraction de nombres constructibles

Soit a et b deux nombres constructibles.

$a + b$ et $a - b$ sont constructibles.

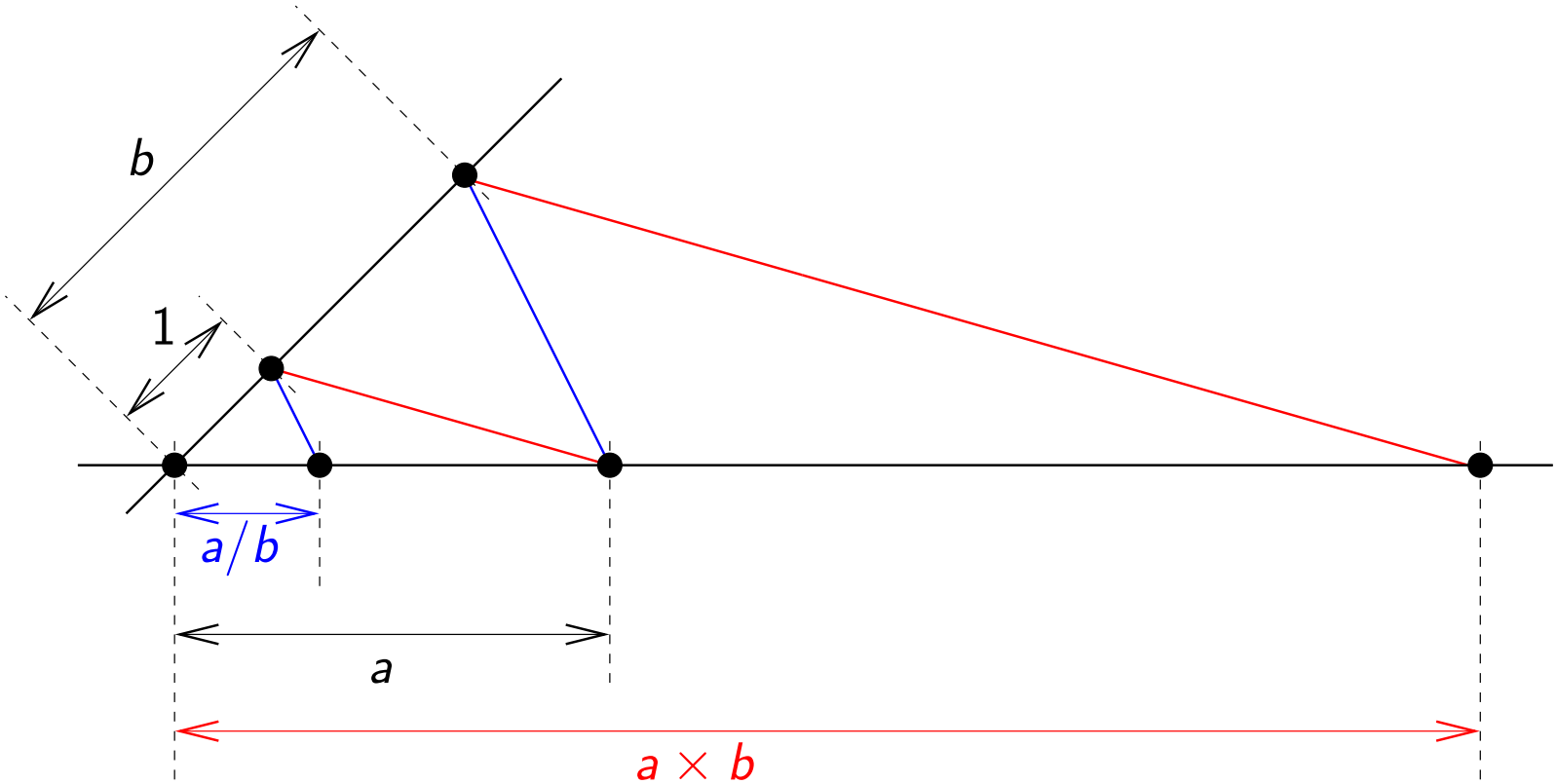


Les **entiers** $(\ldots, -2, -1, 0, 1, 2, \ldots)$ sont **constructibles**.

Multiplication et division de nombres constructibles

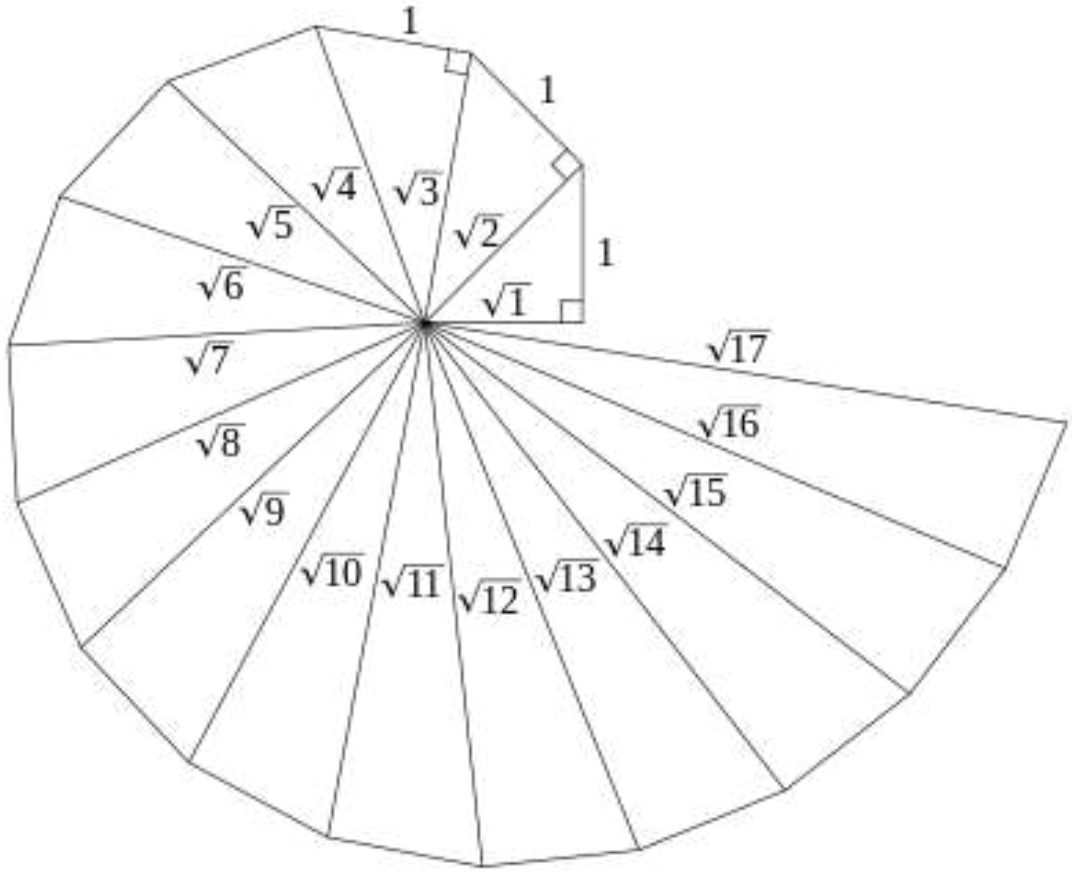
Soit a et b deux nombres constructibles.

$a \times b$ et a/b sont constructibles.



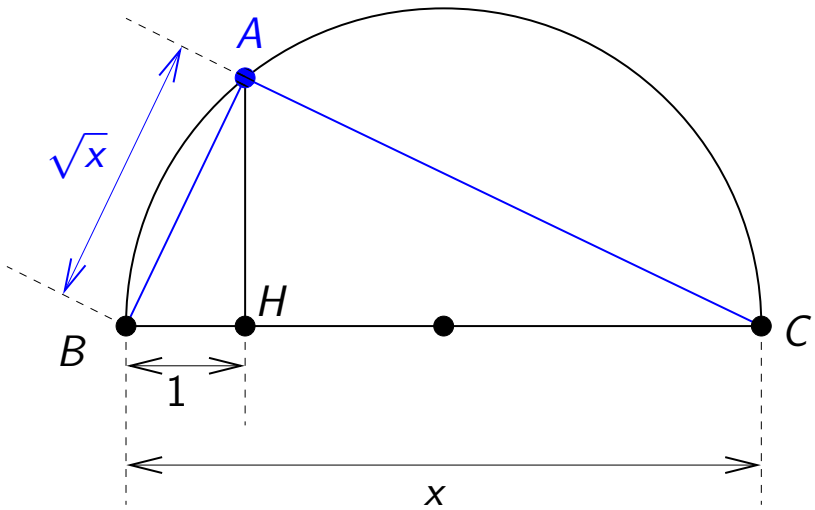
Les **rationnels** (fractions) sont **constructibles**.

Escargot de Pythagore



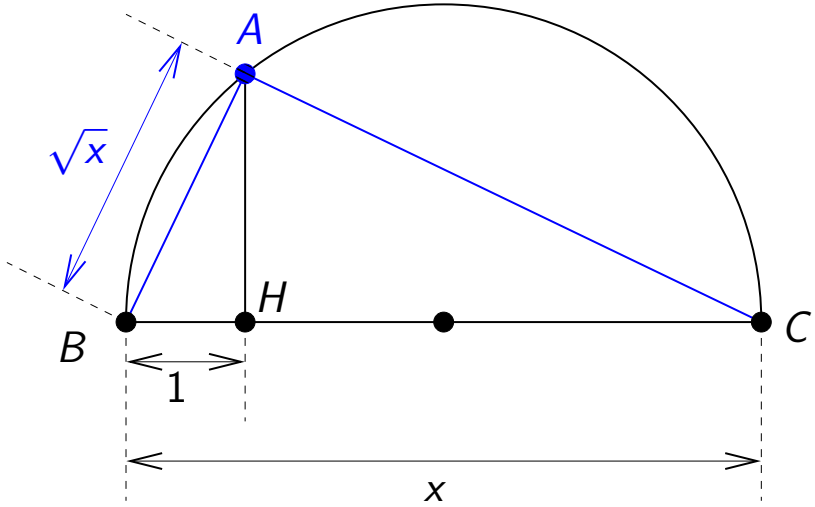
Racine carrée de nombres constructibles

Si x est constructible, alors $\sqrt{x}$ est constructible.



Racine carrée de nombres constructibles

Si x est constructible, alors $\sqrt{x}$ est constructible.



AHB et ABC sont des triangles semblables.

Donc $\frac{AB}{BH} = \frac{BC}{AB}$

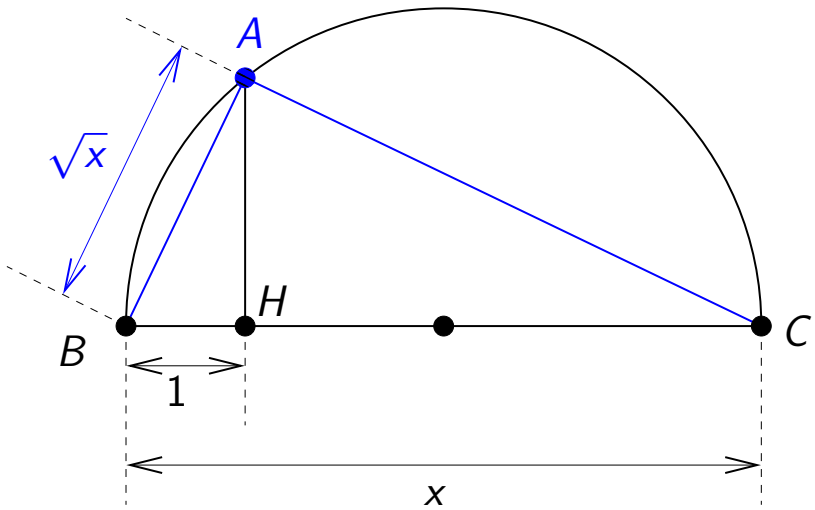
$AB^2 = BC \times BH$

$AB^2 = x$

$AB = \sqrt{x}$

Racine carrée de nombres constructibles

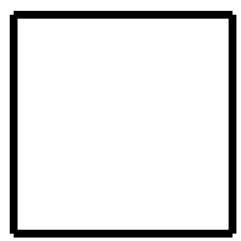
Si x est constructible, alors $\sqrt{x}$ est constructible.



Exemple : $\sqrt[4]{2} = \sqrt{\sqrt{2}}$ ou $3 + \sqrt{27 - \dfrac{\sqrt{23} - 6}{\sqrt{5} - \sqrt[4]{2}}}$ sont constructibles.

Duplication du carré

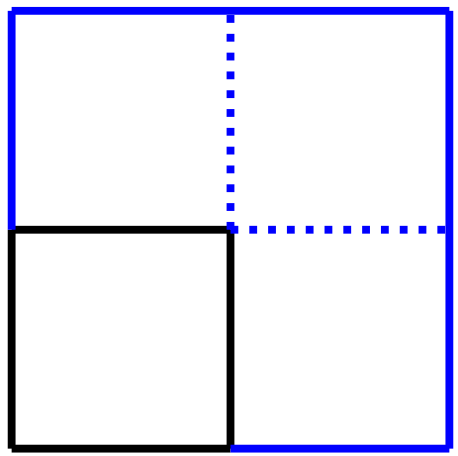
Trouver un **carré dont la surface est double** de celle d'un carré donné.



Duplication du carré

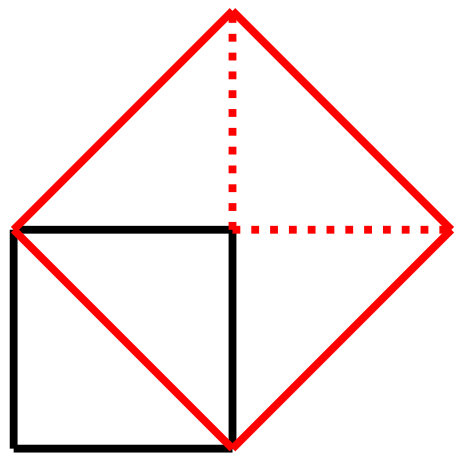
Trouver un **carré dont la surface est double** de celle d'un carré donné.

Doubler la taille des côtés ne convient pas : la surface est quadruplée



Duplication du carré

Trouver un **carré dont la surface est double** de celle d'un carré donné.



Duplication du cube

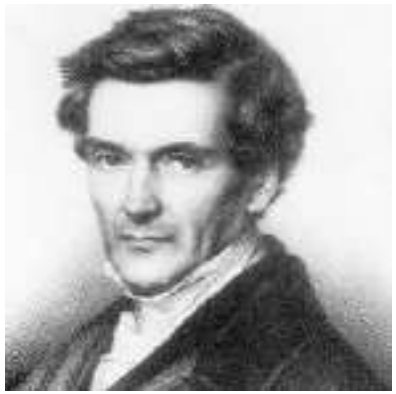
La légende : Les Déliens, victime d'une épidémie de peste, demandèrent à l'oracle de Delphes comment faire cesser cette épidémie. La réponse de l'oracle fut qu'il fallait **doubler** l'autel consacré à Apollon, autel dont la forme était **un cube** parfait.

Comment faire ? ? Cela revient à **construire** $\sqrt[3]{2}$.

$$\sqrt[3]{2} \times \sqrt[3]{2} \times \sqrt[3]{2} = 2$$

Théorème de Wantzel

Pierre-Laurent Wantzel (1837) :
Les nombres constructibles sont les rationnels et les racines de certains polynômes de degré 2^n à coefficients entiers.



P.-L. Wantzel (1814 – 1848)

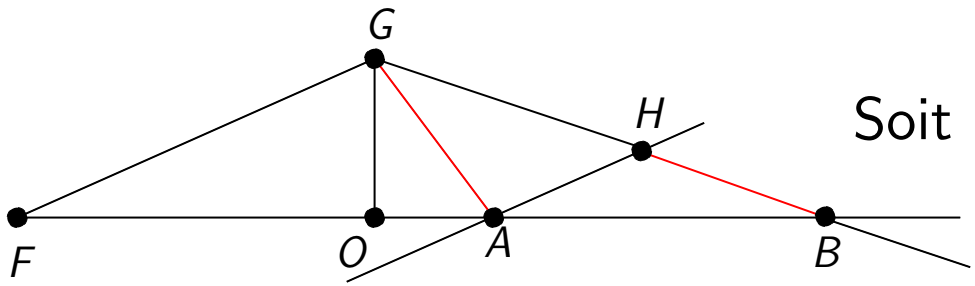
$\sqrt[3]{2}$ est solution racine $x^3 - 2$.

Comme 3 n'est pas une puissance de 2,

$\sqrt[3]{2}$ **n'est pas constructible**.

La duplication du cube est impossible à la règle et au compas.

Construire une racine cubique à la règle graduée et au compas



Soit $OA = d < 1$, $OF = 3d$.

Tracer le triangle rectangle OAG tel que $AG = 1 =$ graduation.

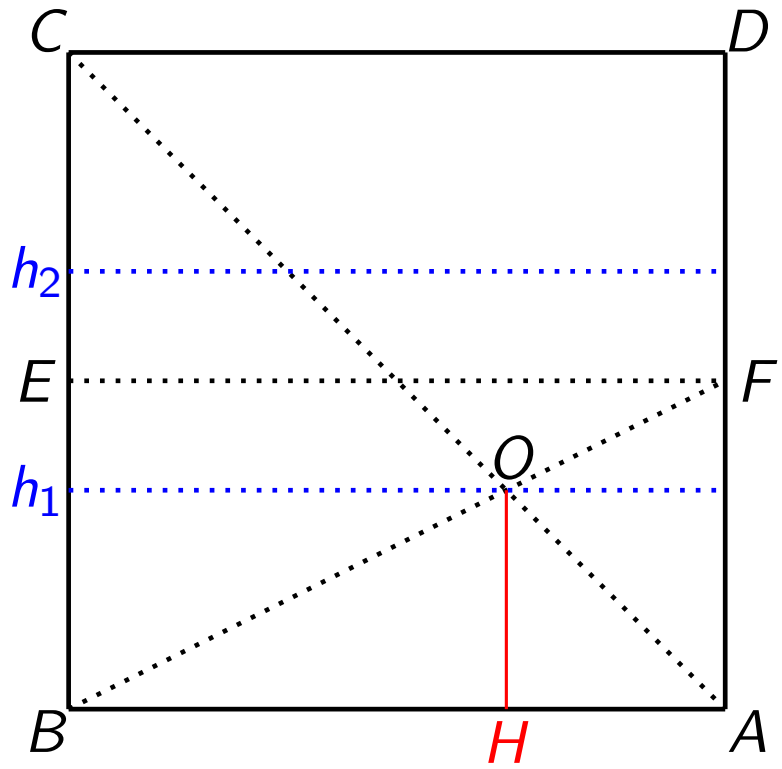
Tracer la parallèle (AH) à (FG) passant par A.

Jusqu'ici tout se fait à la règle et au compas.

Faire passer la règle graduée par G, avec une graduation sur (AH) et sur (OA).

On a alors $AB = 2\sqrt[3]{d}$.

Construire $\sqrt[3]{2}$ par origami



Plier un carré ABCD en trois.

Plier en deux horizontalement
$\Rightarrow$ pli EF.

Plier suivant BF et AC.
Le point d'intersection est O.

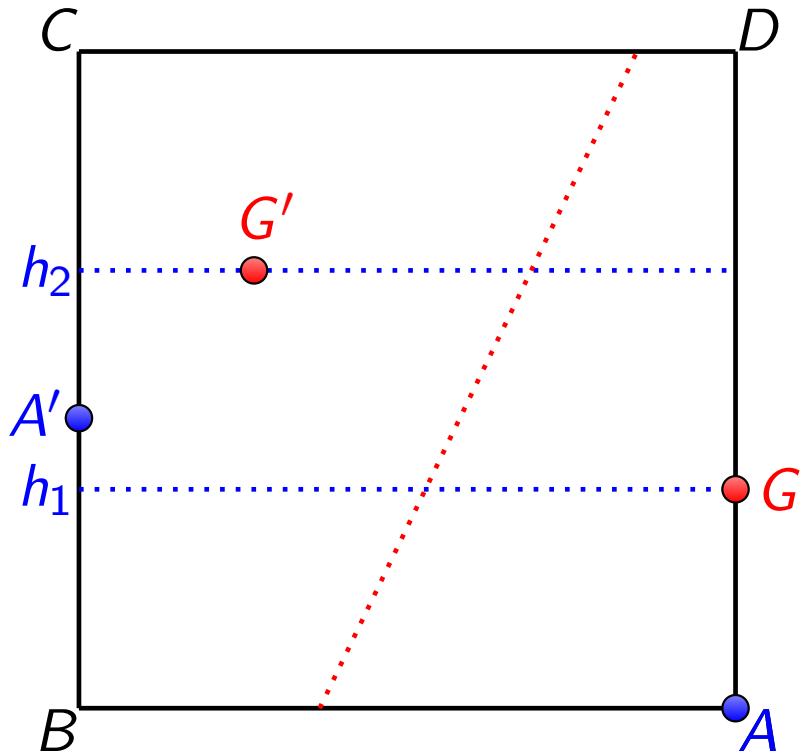
Plier sur l'horizontale h_1
passant par O.

De la même manière,
construire l'horizontale h_2.

Par Thales, $\dfrac{OC}{OA} = \dfrac{BC}{AF} = 2$, donc $OC = 2OA$.

Par Thales, $\dfrac{HO}{BC} = \dfrac{AO}{AC} = \dfrac{AO}{AO + OC} = \dfrac{AO}{3AO} = \dfrac{1}{3}$.

Construire $\sqrt[3]{2}$ par origami



Plier ABCD en trois.

G : intersection de (AD) et h_1.

Plier pour que
A aille sur BC (en A') et
G aille sur h_2 (en G').

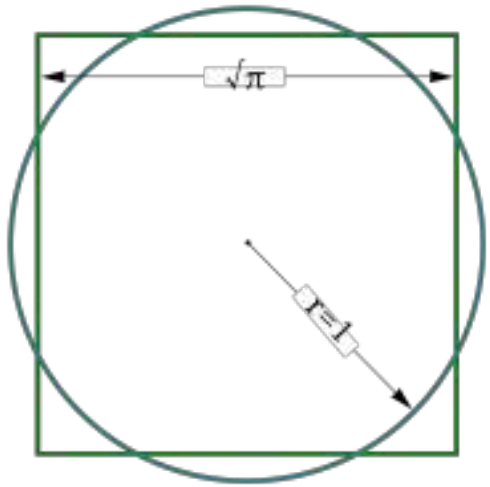
On a alors $\dfrac{CA'}{BA'} = \sqrt[3]{2}$.

Quadrature du cercle

La **quadrature du cercle** consiste à construire un carré de même aire qu'un cercle donné à l'aide d'une règle et d'un compas.

Aire d'un cercle de rayon $r = \pi r^2$.

Cela revient à la **construction** à la règle et au compas de $\sqrt{\pi}$ donc **de π**.



Ce problème apparait sur le papyrus Rhind ($\sim$1650 av. J.-C.) du scribe Ahmès.

Preuve de son **impossibilité** par von Lindemann en 1882 à l'aide du théorème de Wantzel. Il montre que π est transcendant (i.e. racine d'aucun polynôme).

Quadrature du cercle : toujours impossible

La quadrature du cercle ne peut pas être résolue ni avec un compas et une règle graduée, ni par origami.

Cela vient du fait que π est transcendant (i.e. racine d'aucun polynôme).

De nos jours "Chercher la quadrature du cercle" signifie "Tenter de résoudre un problème insoluble".

≪ *Some mathematics problems look simple, and you try them for a year or so, and then you try them for a hundred years, and it turns out that they're extremely hard to solve. There's no reason why these problems shouldn't be easy, and yet they turn out to be extremely intricate.* ≫

Andrew Wiles

Triplets pythagoriciens

Triplet pytagoricien : entiers a,b,c, tels que $a^2 + b^2 = c^2$.
Exemple : 3,4,5 $\quad 3^2 + 4^2 = 9 + 16 = 25 = 5^2$

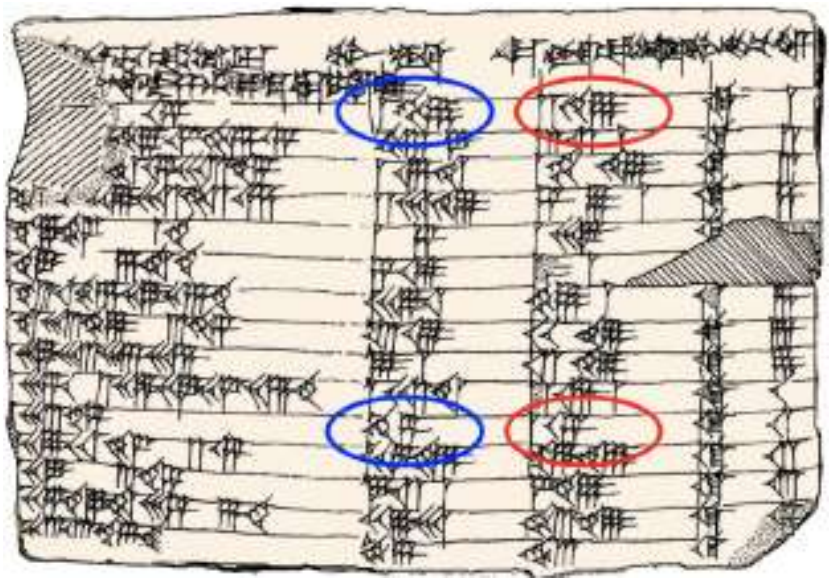
Connus depuis l'antiquité :

Tablette Plimpton 322, vers - 1800

Triplets pythagoriciens

Triplet pytagoricien : entiers a,b,c, tels que $a^2 + b^2 = c^2$.
Exemple : 3,4,5 $\quad 3^2 + 4^2 = 9 + 16 = 25 = 5^2$

Connus depuis l'antiquité :



Tablette Plimpton 322, vers - 1800

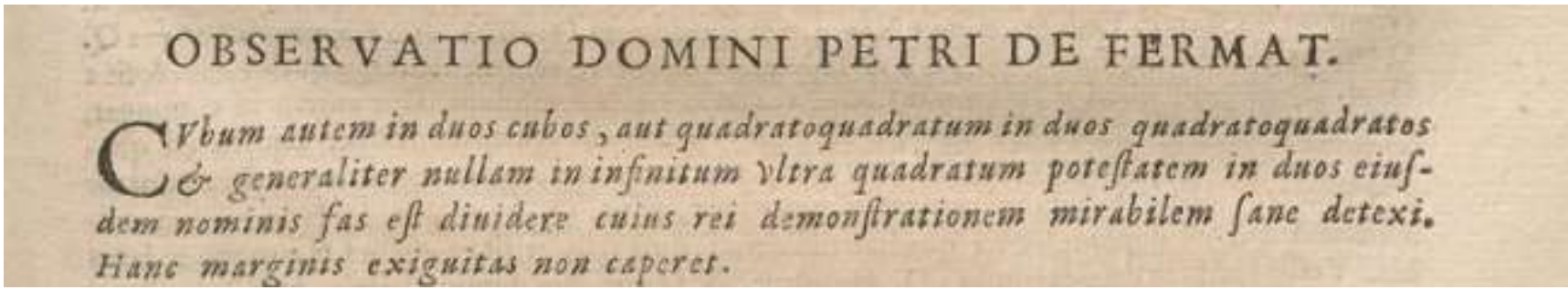
$119^2 + 120^2 = 169^2$

$45^2 + 60^2 = 75^2$

Grand Théorème de Fermat

Pour tout entier $n > 2$, **il n'existe pas** d'entiers strictement positifs a, b et c tels que : $a^n + b^n = c^n$

Pierre de Fermat (∼1605, 1665)



OBSERVATIO DOMINI PETRI DE FERMAT.

Cvbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

Page 61 de la réédition de 1670 par le fils de Fermat du Diophante de Bachet

Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré : j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir.

Approche arithmétique 1650 – 1850

L. Euler (1701–1783)

$\sim$ 1640 : $n = 4$. Fermat.

1753 : $n = 3$. Euler.

1816 : Académie des sciences offre médaille d'or + 3 000 francs.
($\sim$ 2 millions d'euros actuels.)

$\sim$ 1820. Réduction des cas par Germain.

1825 : $n = 5$. Dirichlet et Legendre.

1832 : $n = 14$. Dirichlet.

1847 : $n = 7$. Lamé.

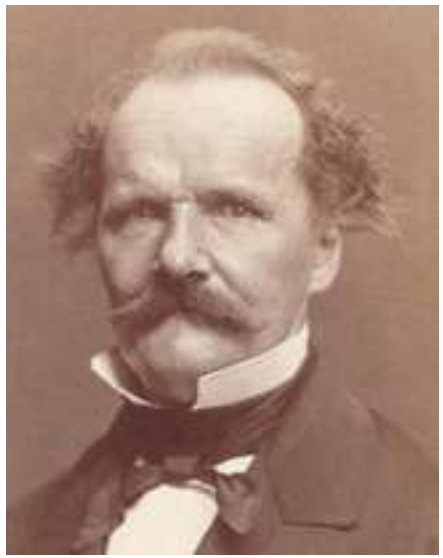
J. P. G. Lejeune Dirichlet (1805–1859)

S. Germain (1776–1831)

1847 : Lamé et Cauchy (indépendamment) présentent une démonstration incomplète. $\rightarrow$ **sans issue.**

Approche algébrique

1847 : *n* **premier régulier**. Kummer.
3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 43, 47, 53, 61, 71, 73, 79, 83, 89, 97, 107, 109, 113, 127, 137, 139, 151, 163, 167, 173, 179, 181, 191, 193, 197, 199, . . .


Ernst Kummer (1810-1893)

Reste les premiers irréguliers : 37, 59, 67, 101, . . .

1850 : Prix de Académie renouvelé.

1850 – 1970

rien

Un peu de géométrie

Triplet pythagoricien : $a^2 + b^2 = c^2$ pour a, b, c entiers

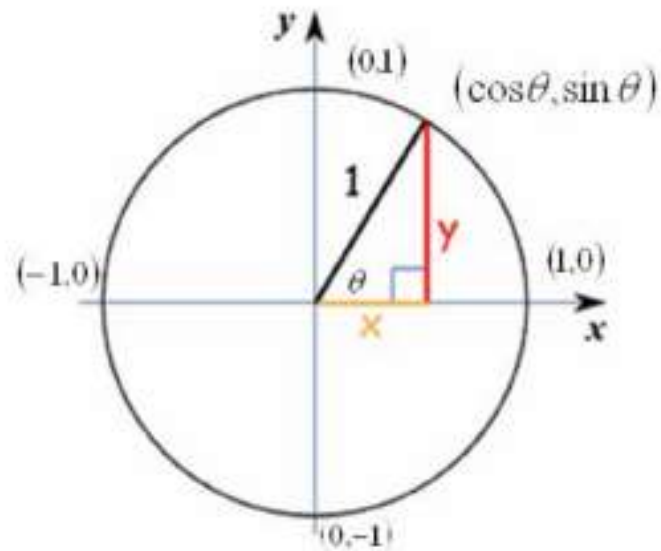
$$\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$$

Posons $x = a/c$ et $y = b/c$,

$$x^2 + y^2 = 1$$ pour x et y rationnels.

La courbe d'équation $x^2 + y^2 = 1$ est le **cercle unitaire**.

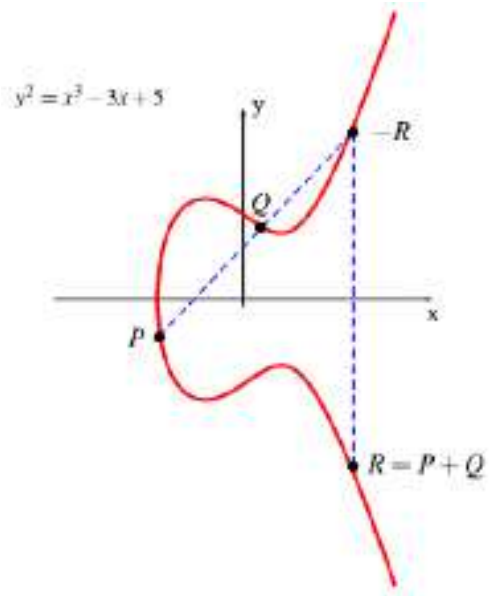
Les triplets pythagoriciens correspondent aux **points** de ce cercle **à coordonnées rationnelles**.



Courbes elliptiques et formes modulaires

courbe elliptique : courbe algébrique, munie entre autres propriétés d'une addition sur ses points.

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$



forme modulaire : fonction du demi-plan dans $\mathbb{C}$ ayant des propriétés de symétrie et de croissance.

Conjecture de Taniyama-Shimura - Weil

Yutaka Taniyama (1927 -1958)

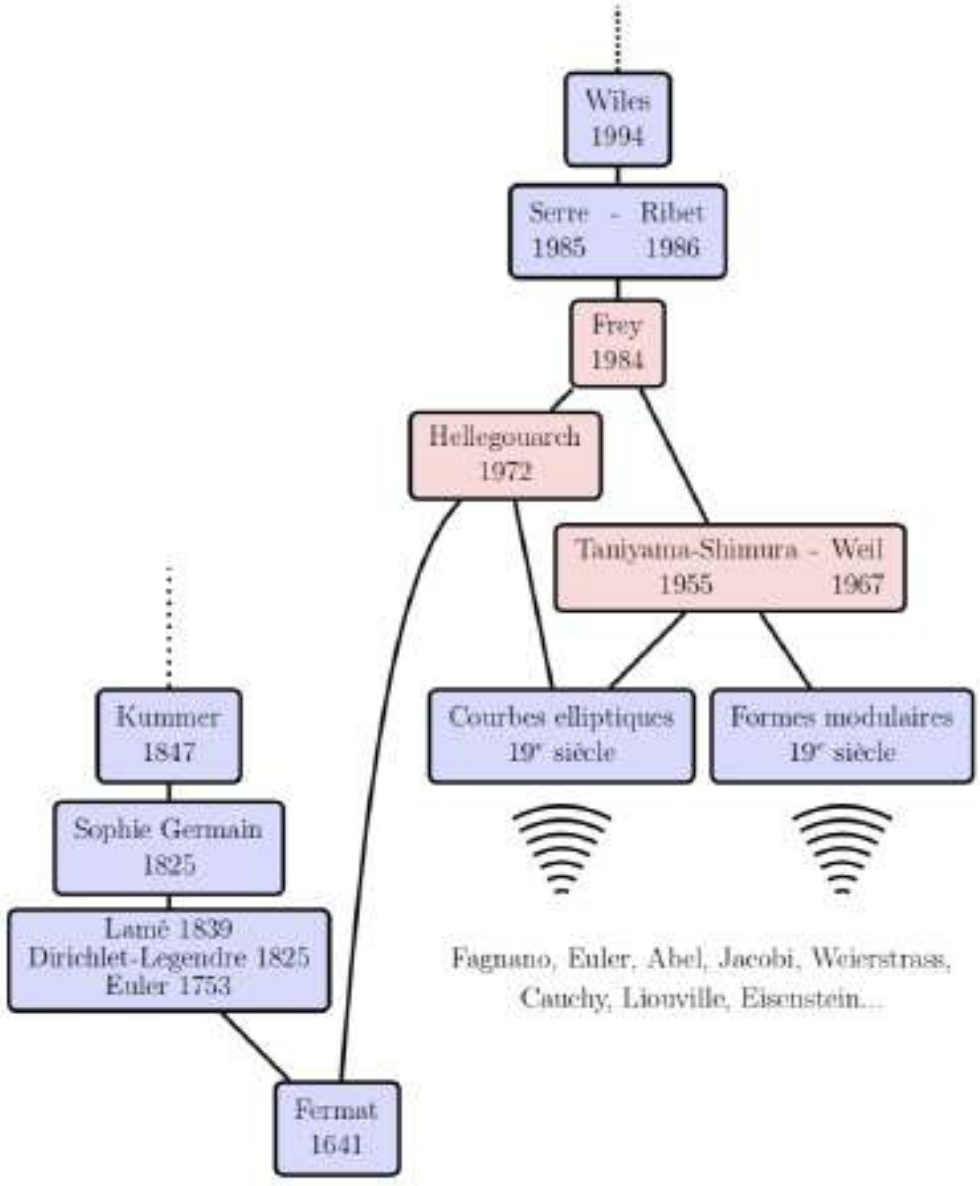
Goro Shimura (1930 -)

André Weil (1906 -1998)

Conjecture Shimura -Taniyama, 1955 – Weil, 1967

Pour toute **courbe elliptique** sur $\mathbb{Q}$, la fonction associée est une **forme modulaire** (parabolique normalisée de poids 2).

Vers la preuve du Théorème de Fermat



Un schéma de preuve

1) Si $a^n + b^n = c^n$ **a des solutions pour** $n > 2$, alors **la courbe elliptique d'Hellegouarch** C d'équation $y^2 = x(x - a^n)(y + b^n)$ existerait.

2) Si on démontre la conjecture de Shimura-Taniyama-Weil, alors la fonction associée Ã toute courbe elliptique **est une forme modulaire**.

3) Or, la fonction associée la courbe elliptique C **n'est pas une forme modulaire**. **Contradiction**

Donc notre supposition est fausse. Le théorème de Fermat est vrai.

≪ *There's also some sense of freedom. I was so obsessed by this problem that I was thinking about it all the time - when I woke up in the morning, when I went to sleep at night and that went on for eight years.* ≫

Andrew Wiles

Histoire de la preuve de Wiles

Andrew Wiles (1953 -)

- **1986–1988** : **immersion** dans le problème. Bibliographie.
- **1989** : **première stratégie**, via théorie d'Iwazawa.
- **1991** : **changement de stratégie**, utilisation de Flach-Lolyvagin.
- **1993** : **changement d'orientation** vers une autre famille de courbes elliptiques.
- **Juin 1993** : **annonce de la preuve.**
- **Été 1993** : une **erreur profonde** est détectée par Nick Katz et Luc Illusie ! !

Histoire de la preuve de Wiles

- **Début 1994** : Wiles demande l'aide de Richard Taylor, un de ses élèves.
- **Eté 1994** : Wiles et Taylor commence à perdre confiance et se prépare à admettre l'échec.
- **Septembre 1994** : Taylor propose de revenir à Flach-Lolyvagin. Wiles accepte pour montrer que c'est une impasse.

  ≪ *In a flash, I saw that all the things that kept Flach-Lolyvagin from working were what would make the Iwasawa method work.* ≫
- **Octobre 1994** : **annonce de la preuve.**

Histoire de la preuve de Wiles

2 articles :

A. Wiles : Modular elliptic curves and Fermat's Last Theorem,

Ann. of Math. 141 (1995), 443-551.

R. Taylor et A. Wiles : Ring theoretic properties of certain Hecke algebras,

Ann. of Math. 141 (1995), 553-572.

≪ *That particular odyssey is now over. My mind is now at rest.* ≫ A. Wiles

Problème des 4 couleurs : colorer une carte

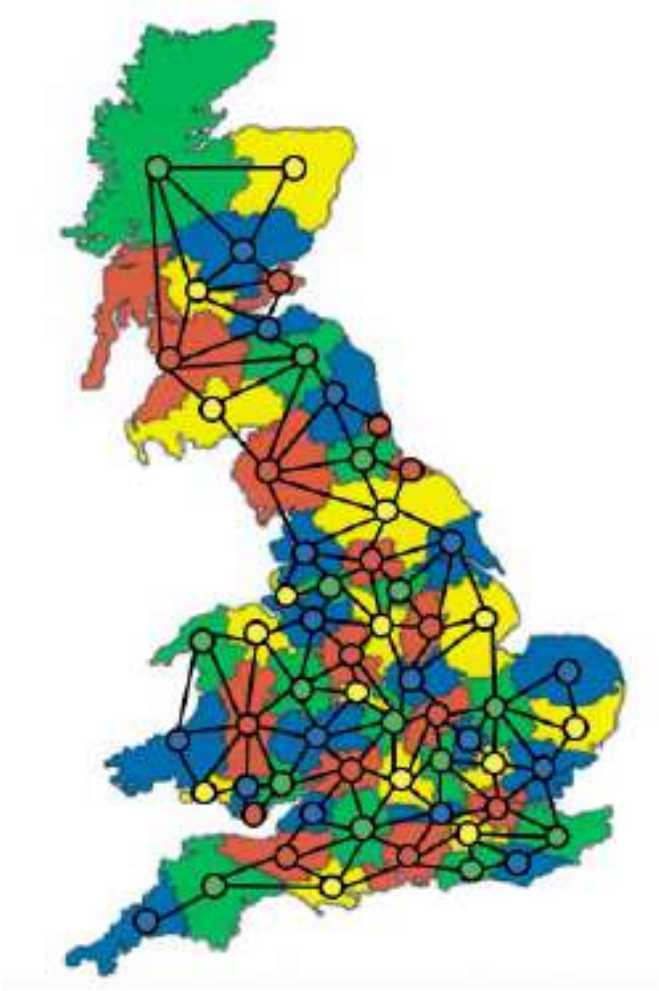
1852, Francis Guthrie : Peut-on colorer les régions (connexes) d'une carte avec 4 couleurs de manière à ce que deux régions voisines (ayant une frontière en commun) aient des couleurs différentes ?

Problème des 4 couleurs : colorer un graphe planaire

Un sommet dans chaque région.
Deux sommets reliés si les régions sont voisines.

Problème des 4 couleurs : colorer un graphe planaire

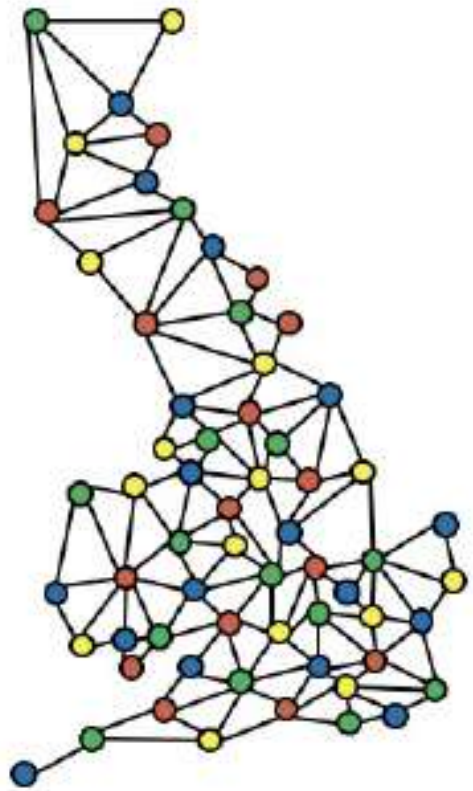
Un sommet dans chaque région.
Deux sommets reliés si les régions sont voisines.



Problème des 4 couleurs : colorer un graphe planaire

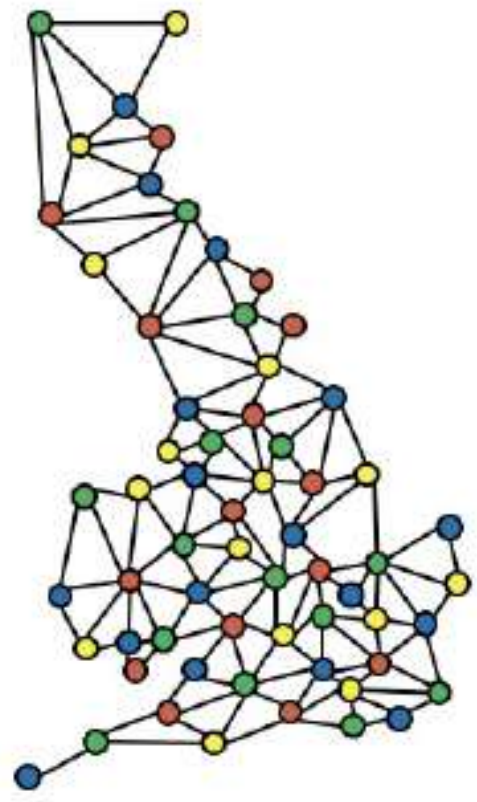
Un sommet dans chaque région.
Deux sommets reliés si les régions sont voisines.

On obtient un **graphe planaire**.



Problème des 4 couleurs : colorer un graphe planaire

Colorer les régions = colorer le graphe planaire.
Donner des couleurs aux sommets telles que deux sommets adjacents aient des couleurs différentes.



Problème des 4 couleurs : premières tentatives

Alfred Kempe (1849 -1922)

Peter G. Tait (1831 -1901)

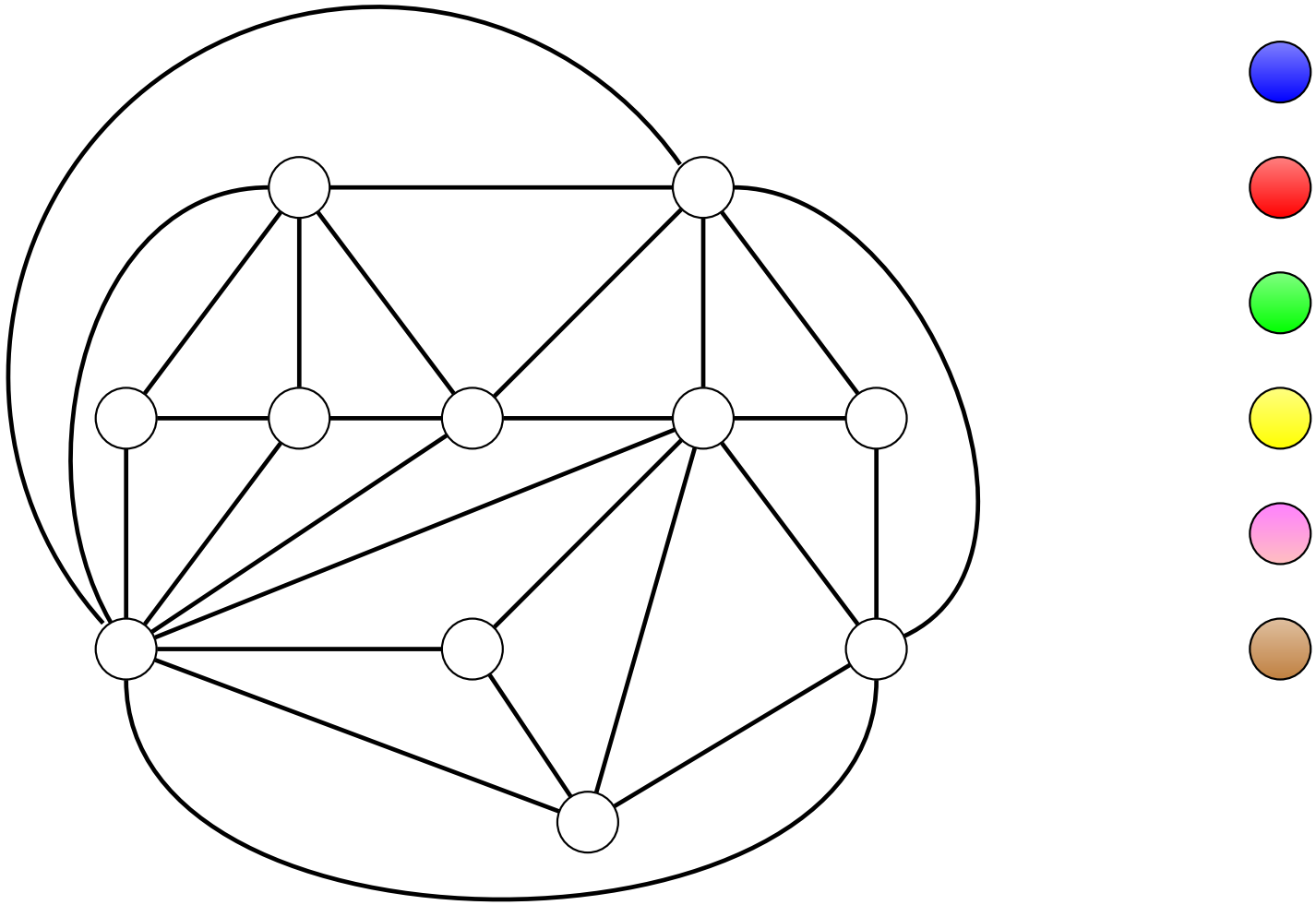
Alfred Kempe en 1879 et Peter G. Tait en 1880 donne une preuve. Des erreurs sont trouvées par Percy Heawood (1890) et Julius Petersen (1891).

Percy J. Heawood (1861 -1955)

Julius Petersen (1839 -1910)

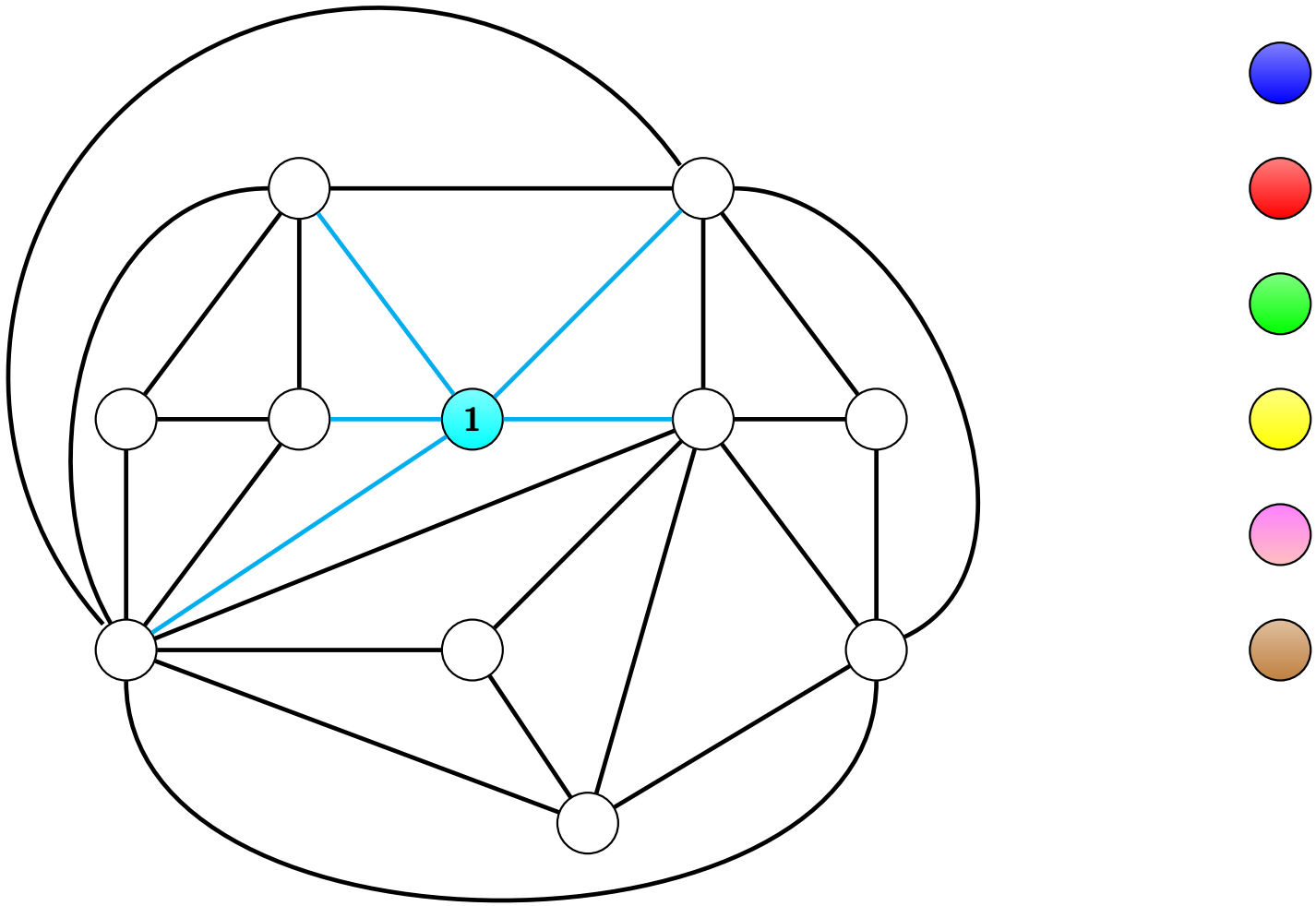
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



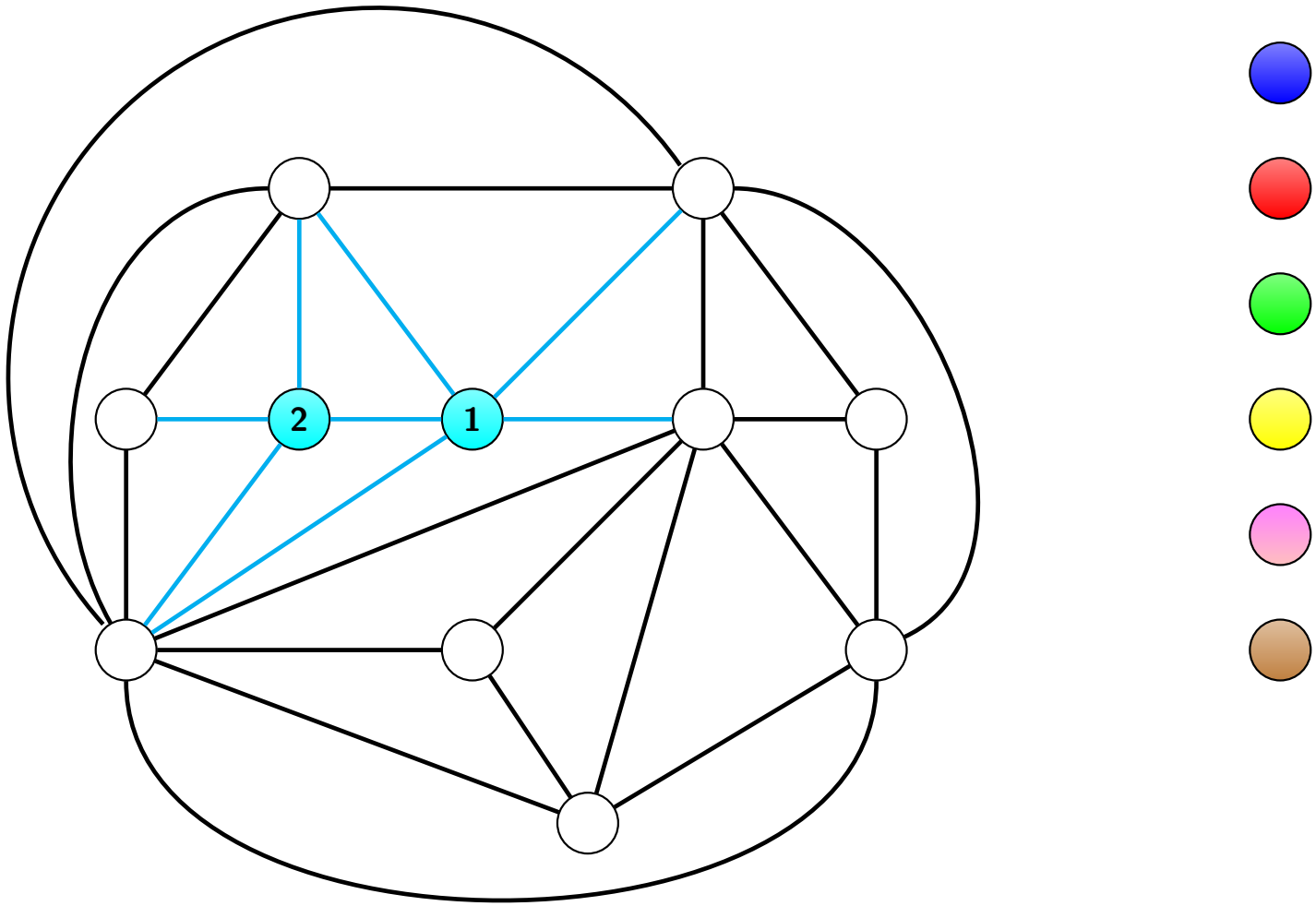
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



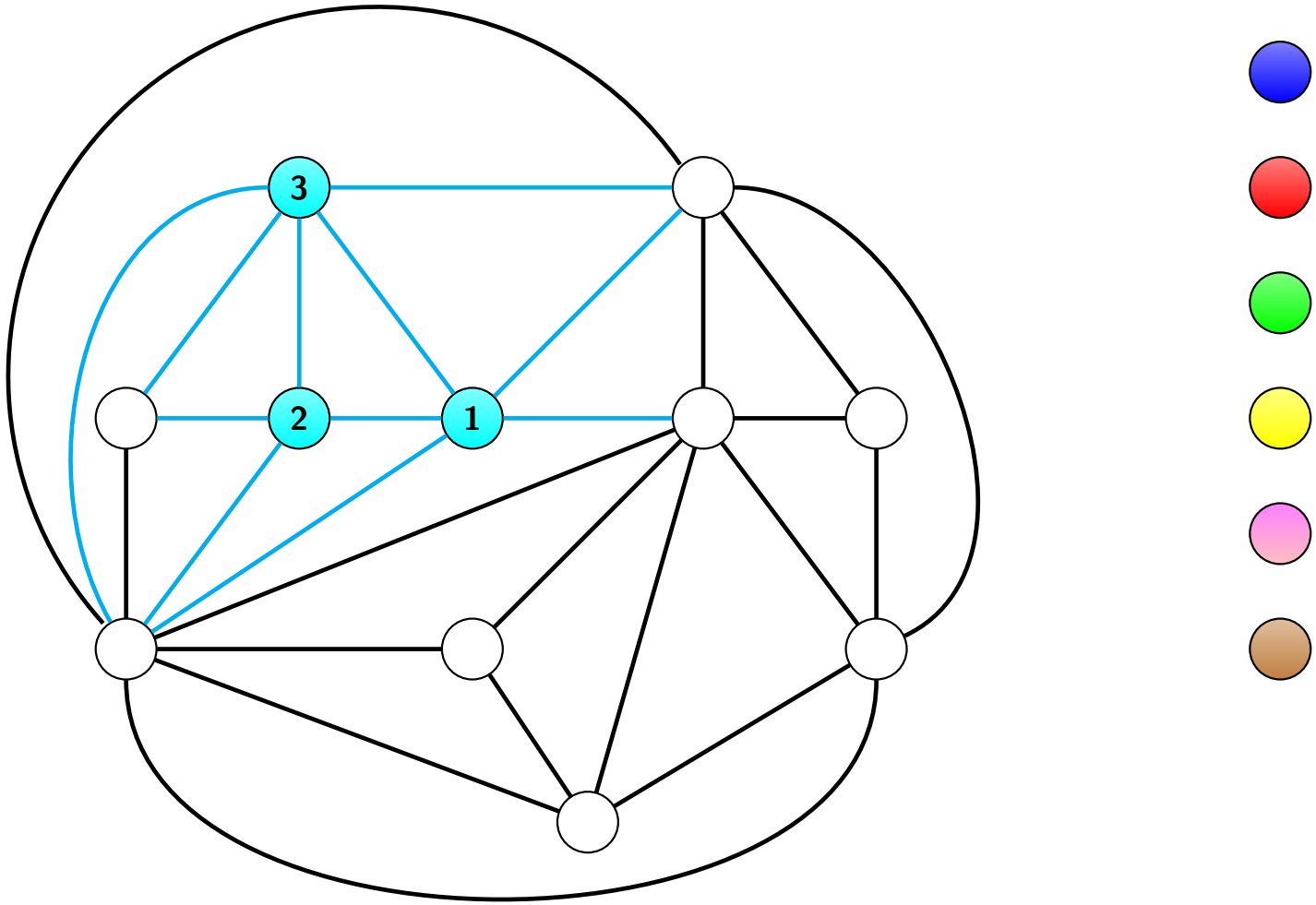
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



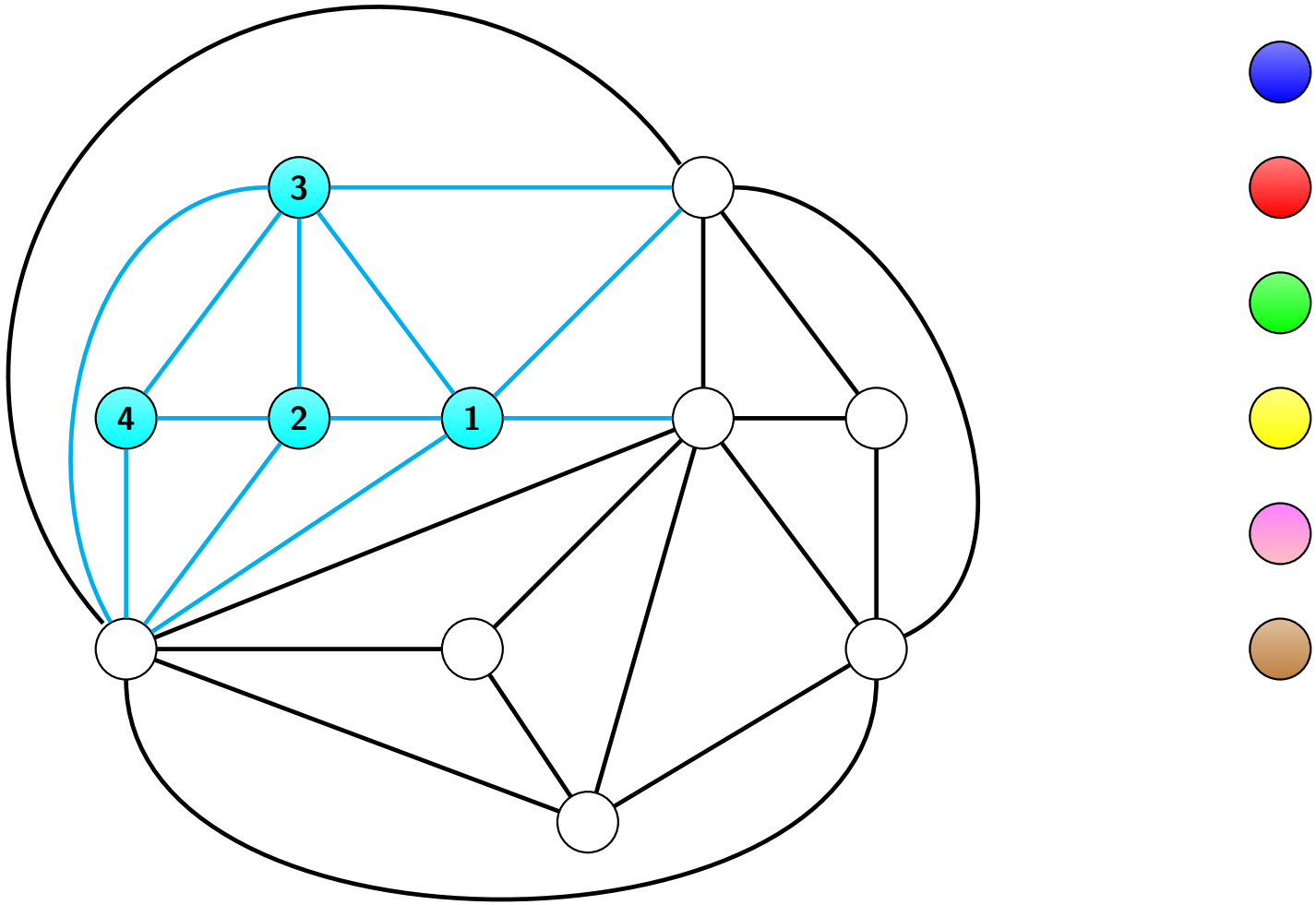
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



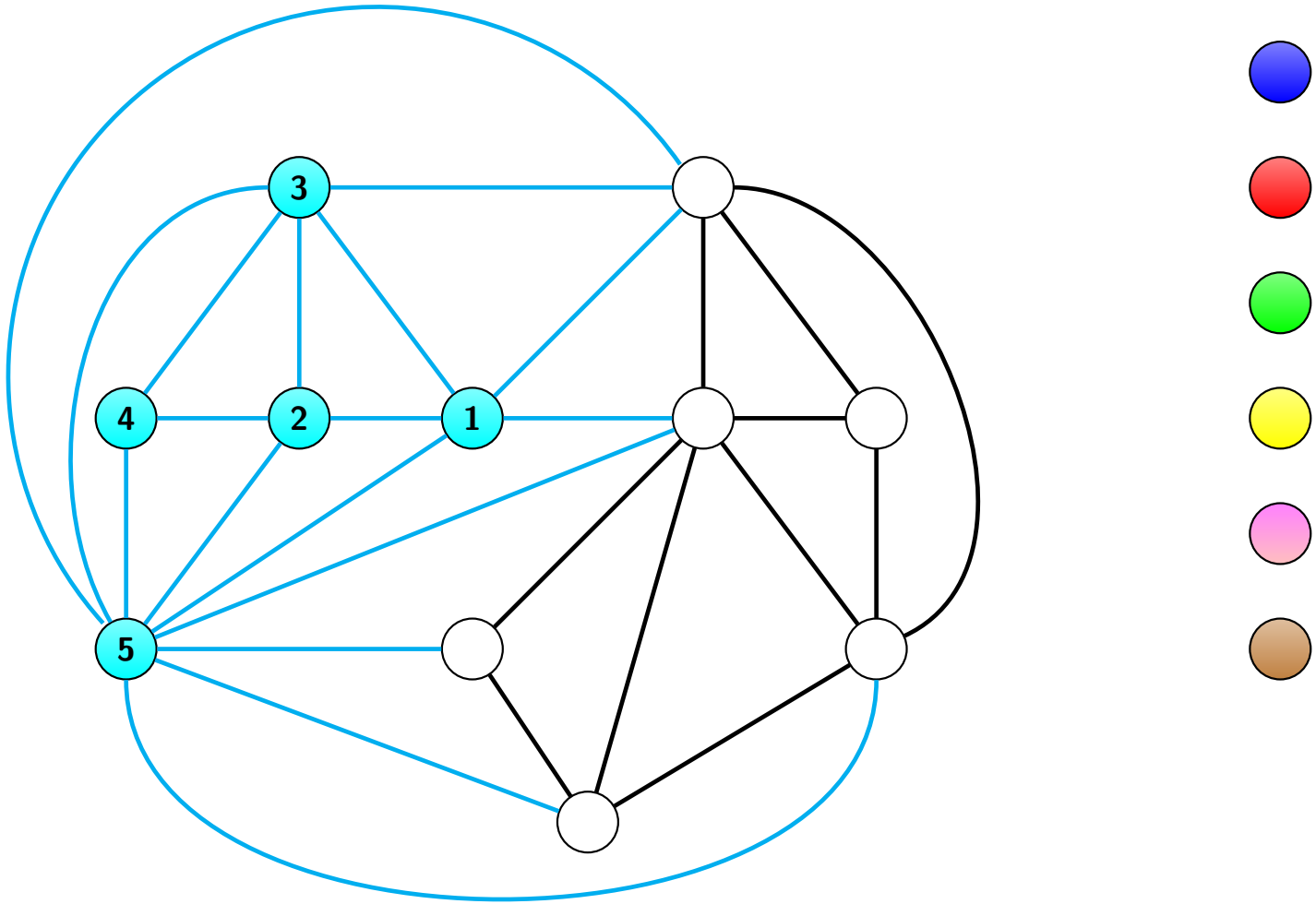
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



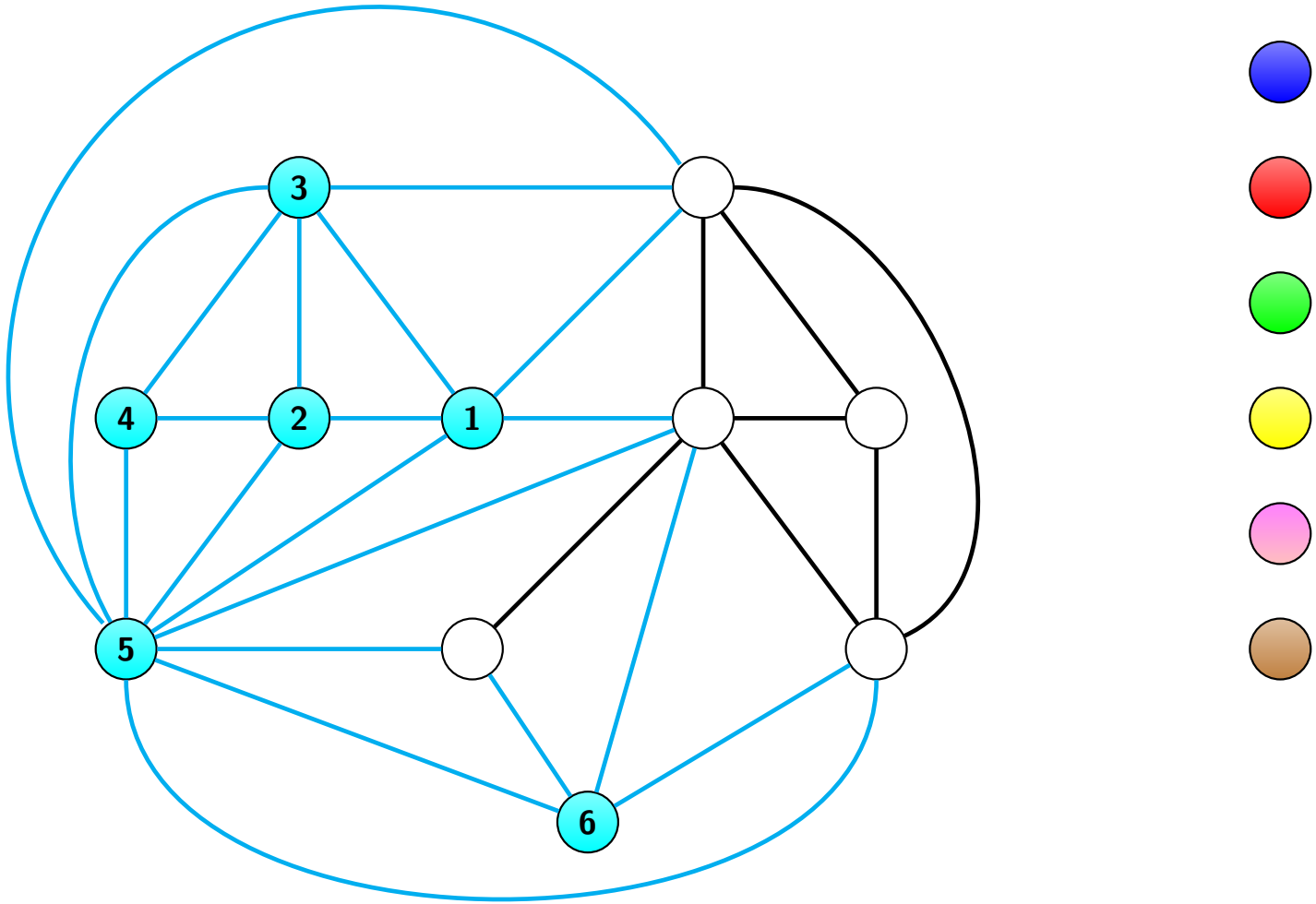
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



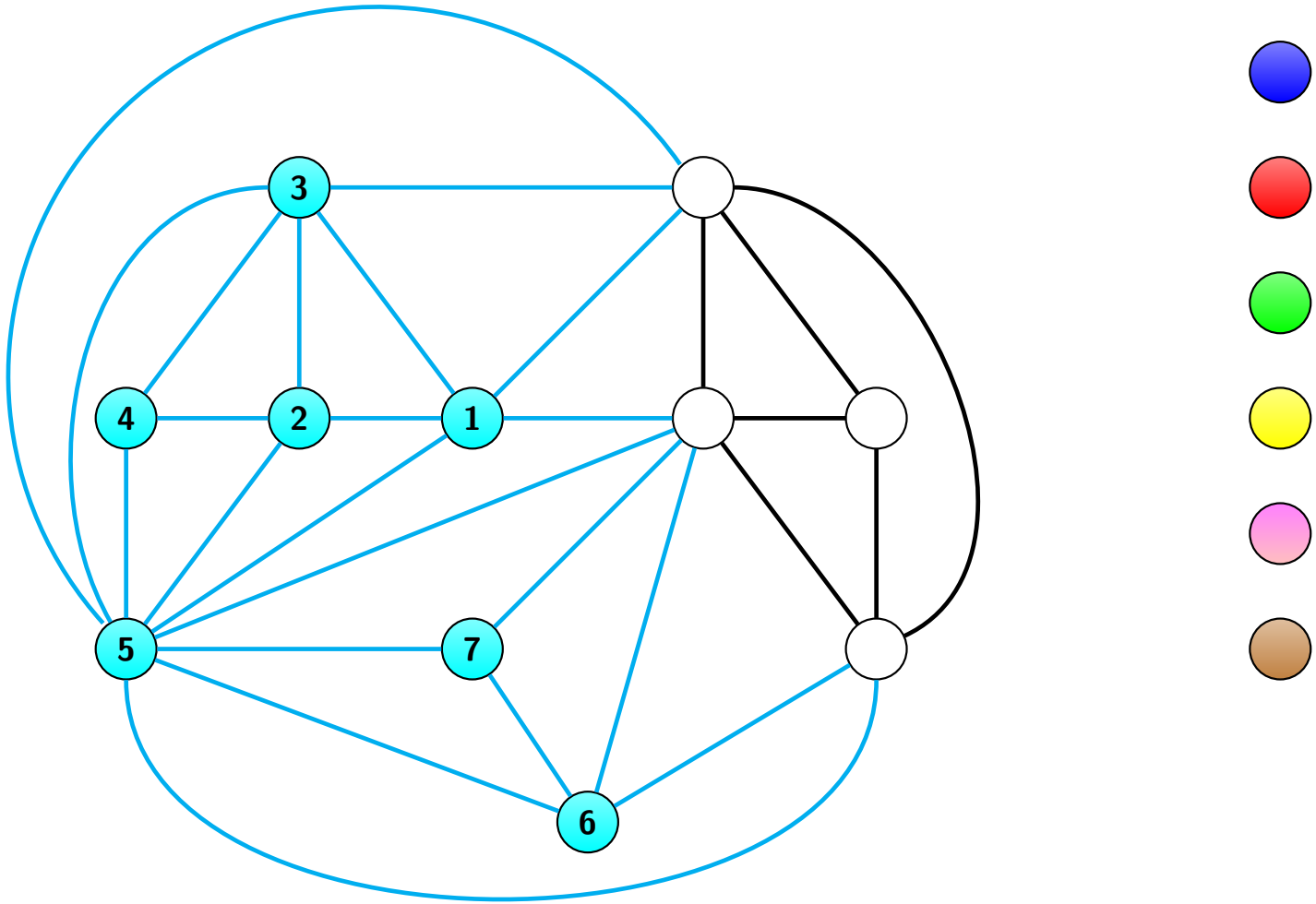
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



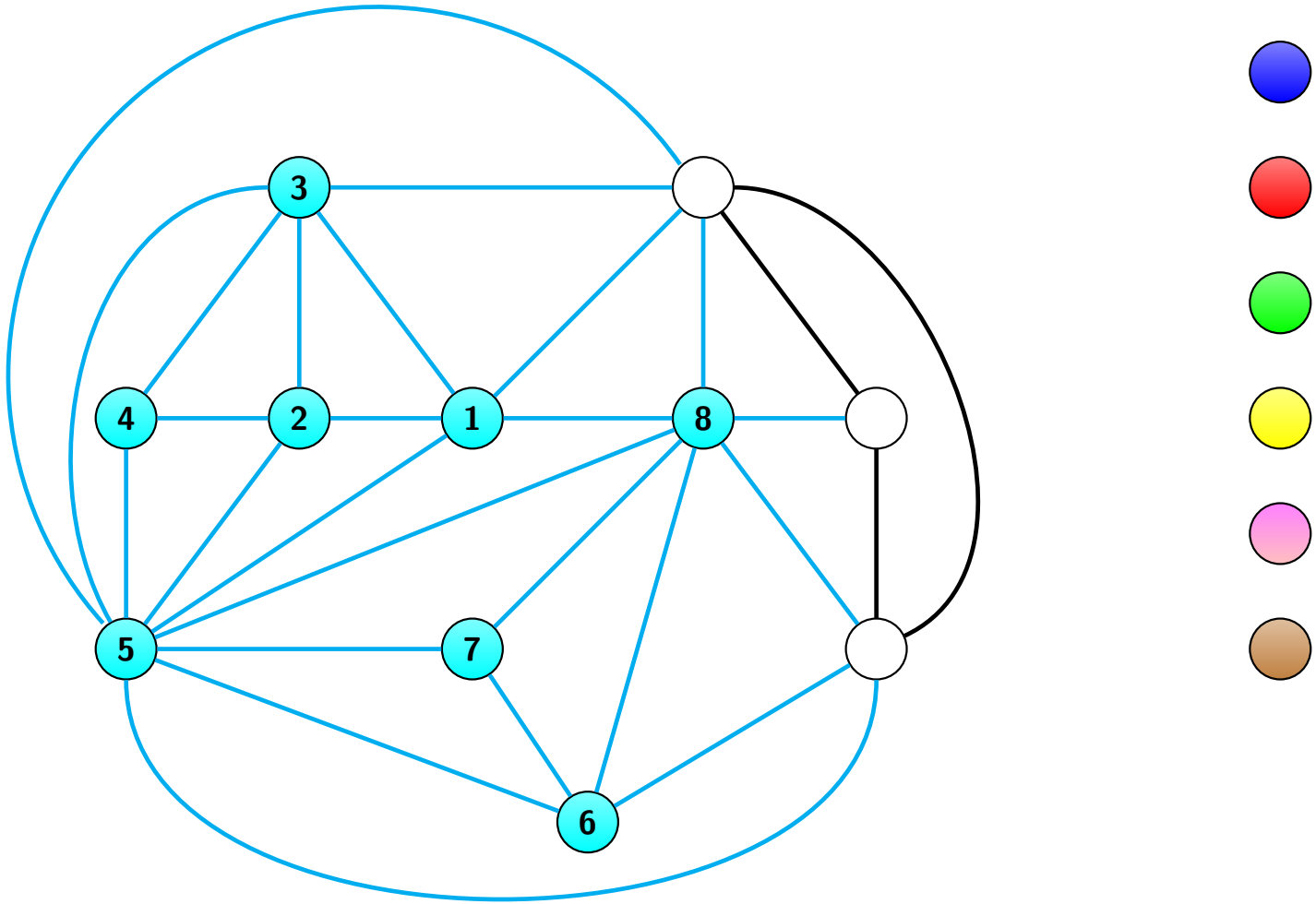
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



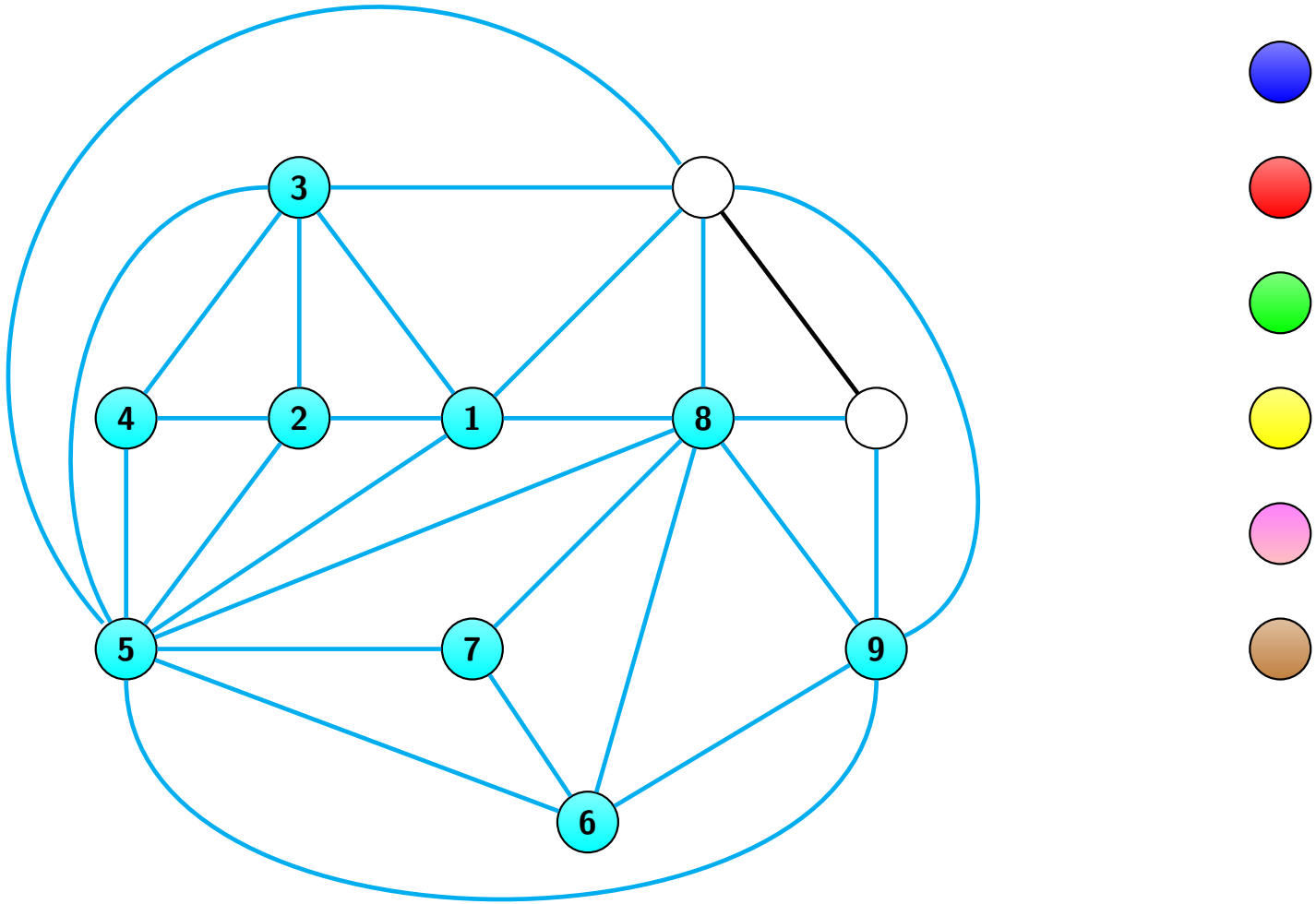
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



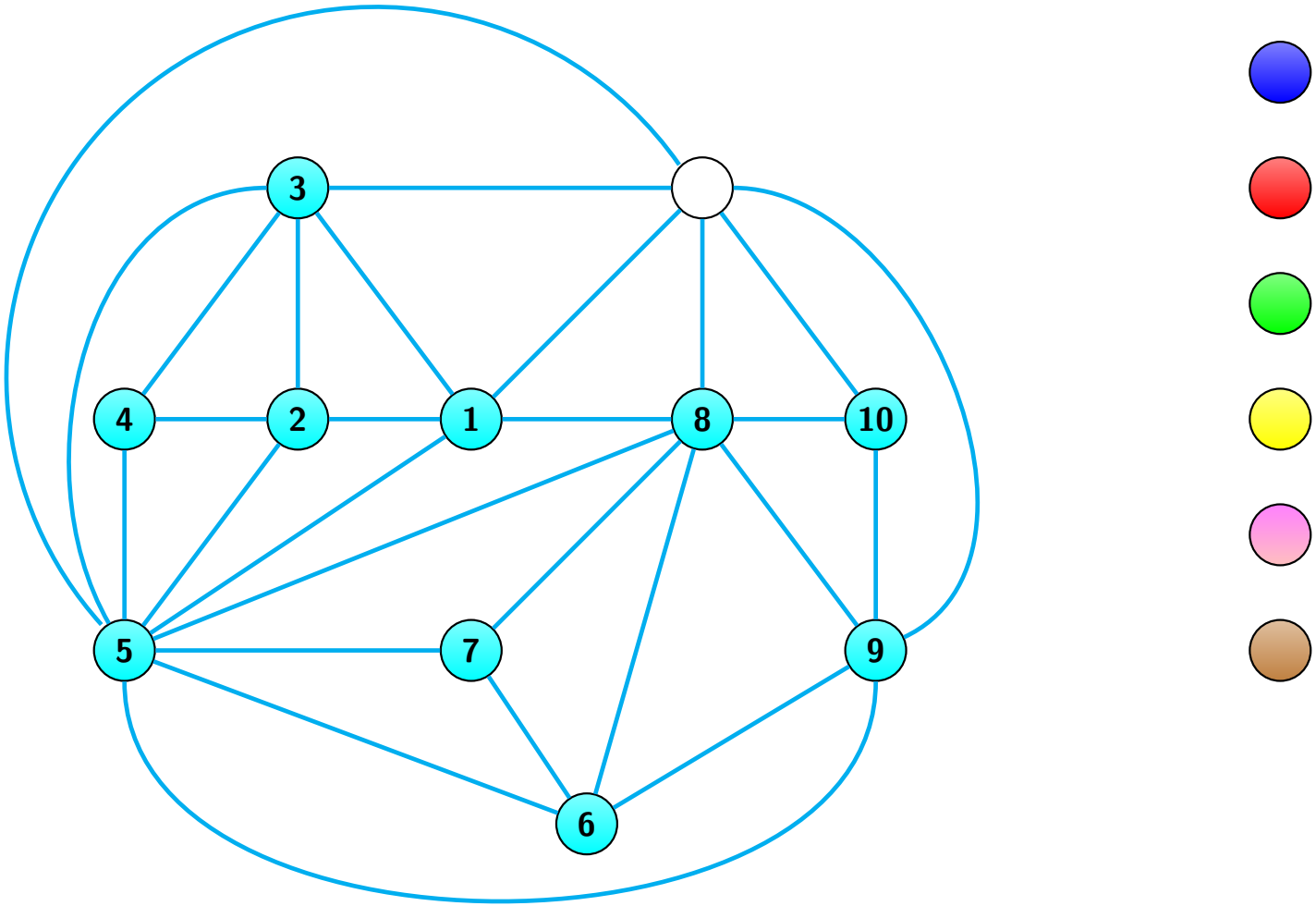
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



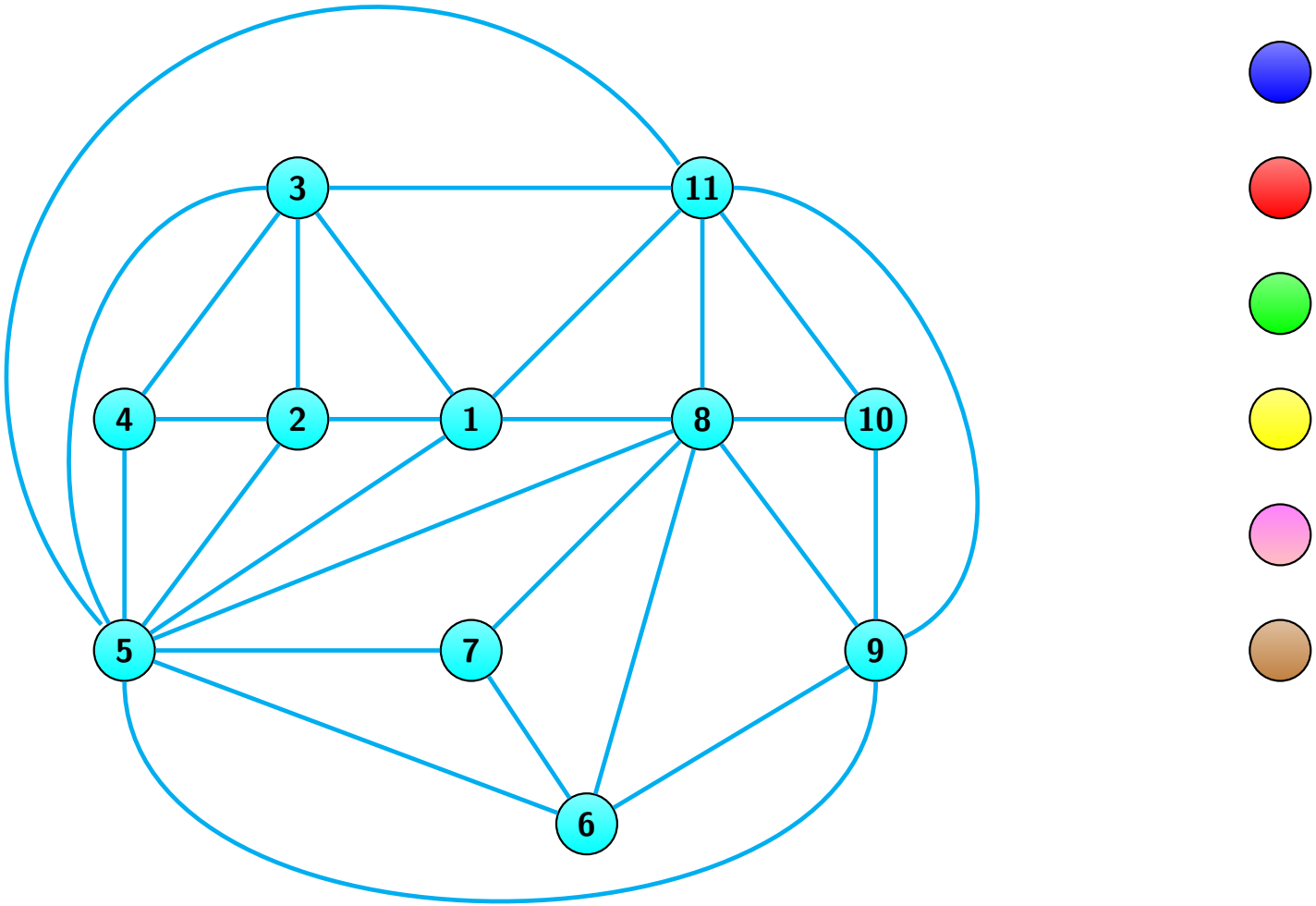
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



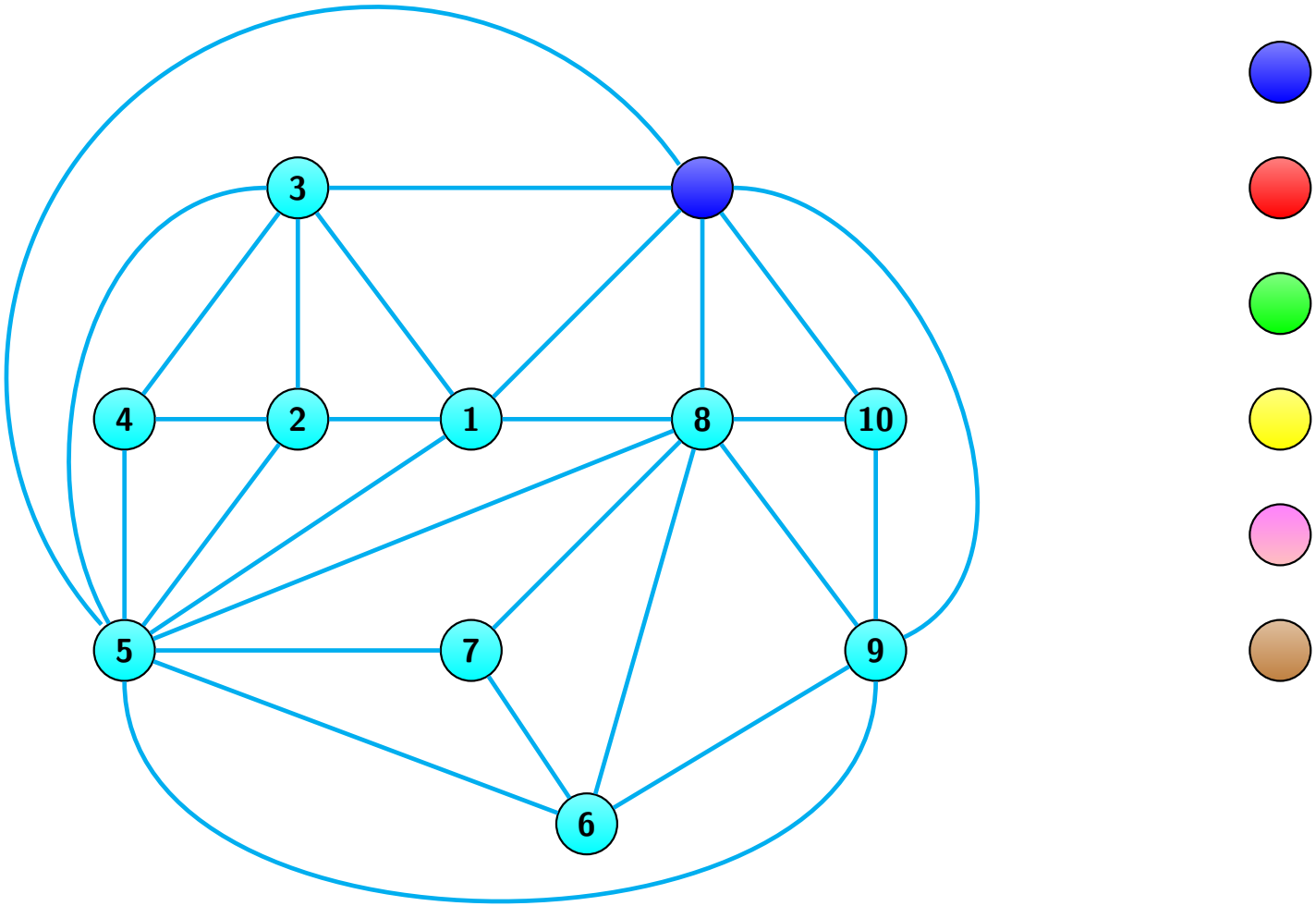
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



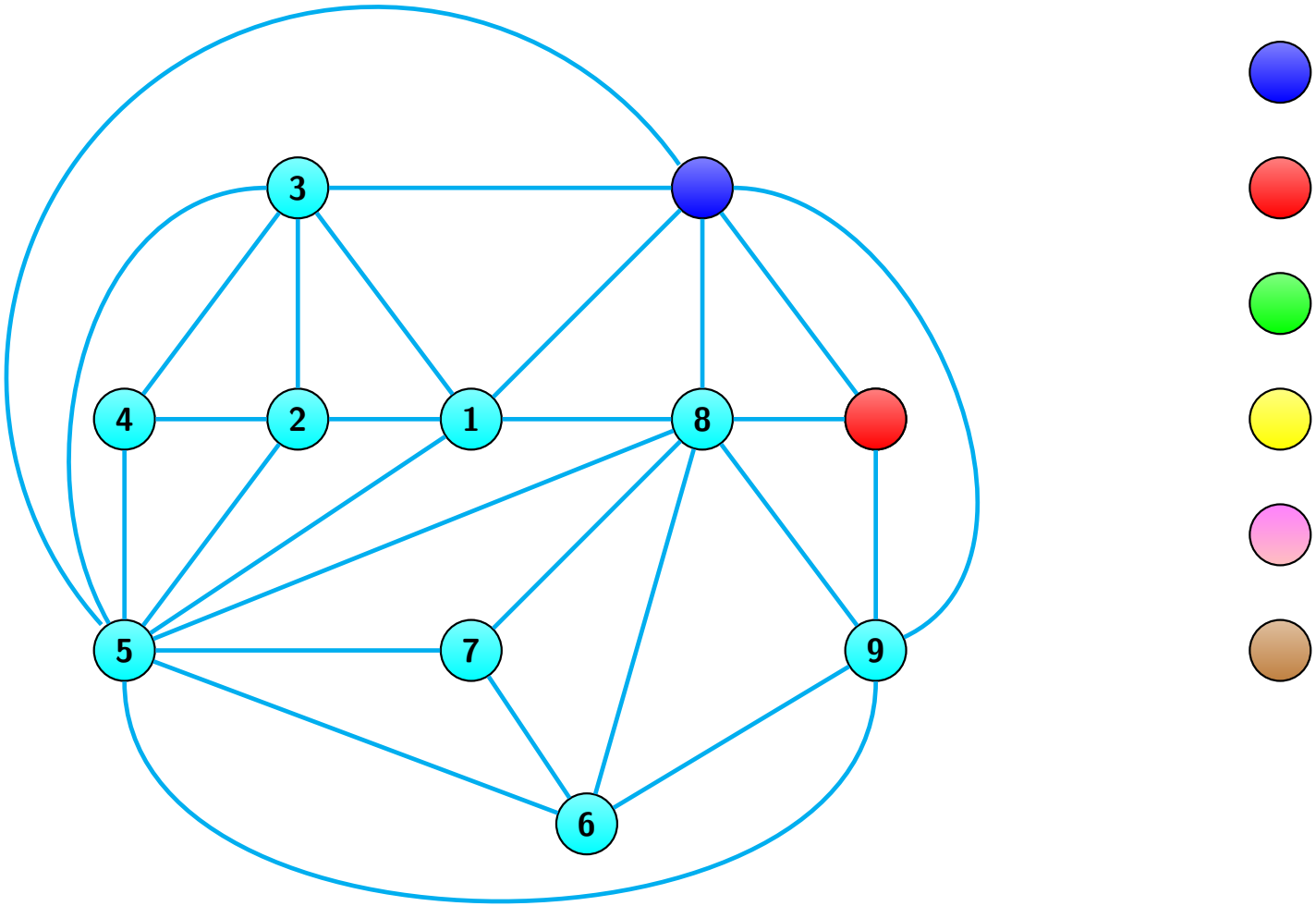
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



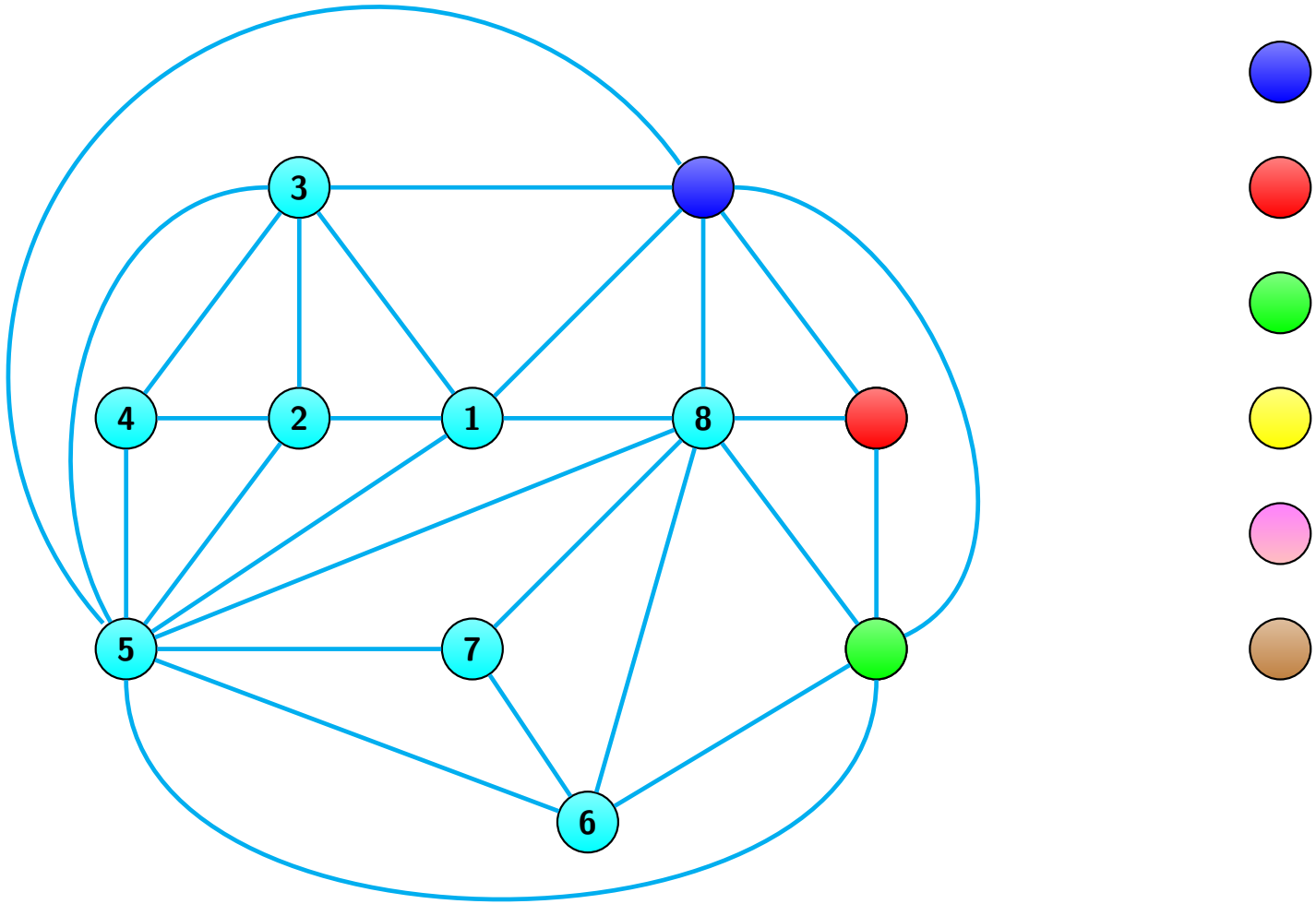
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



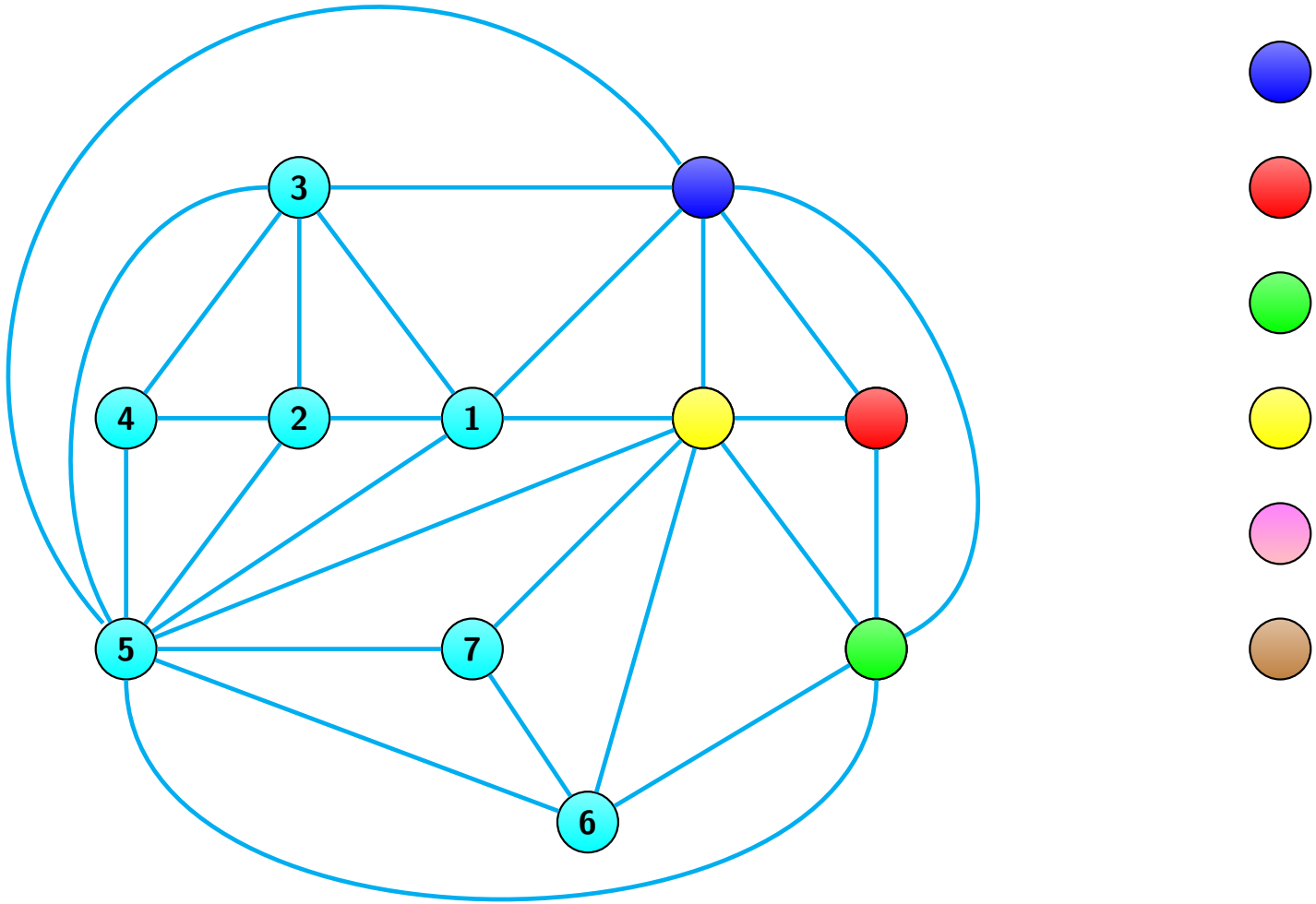
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



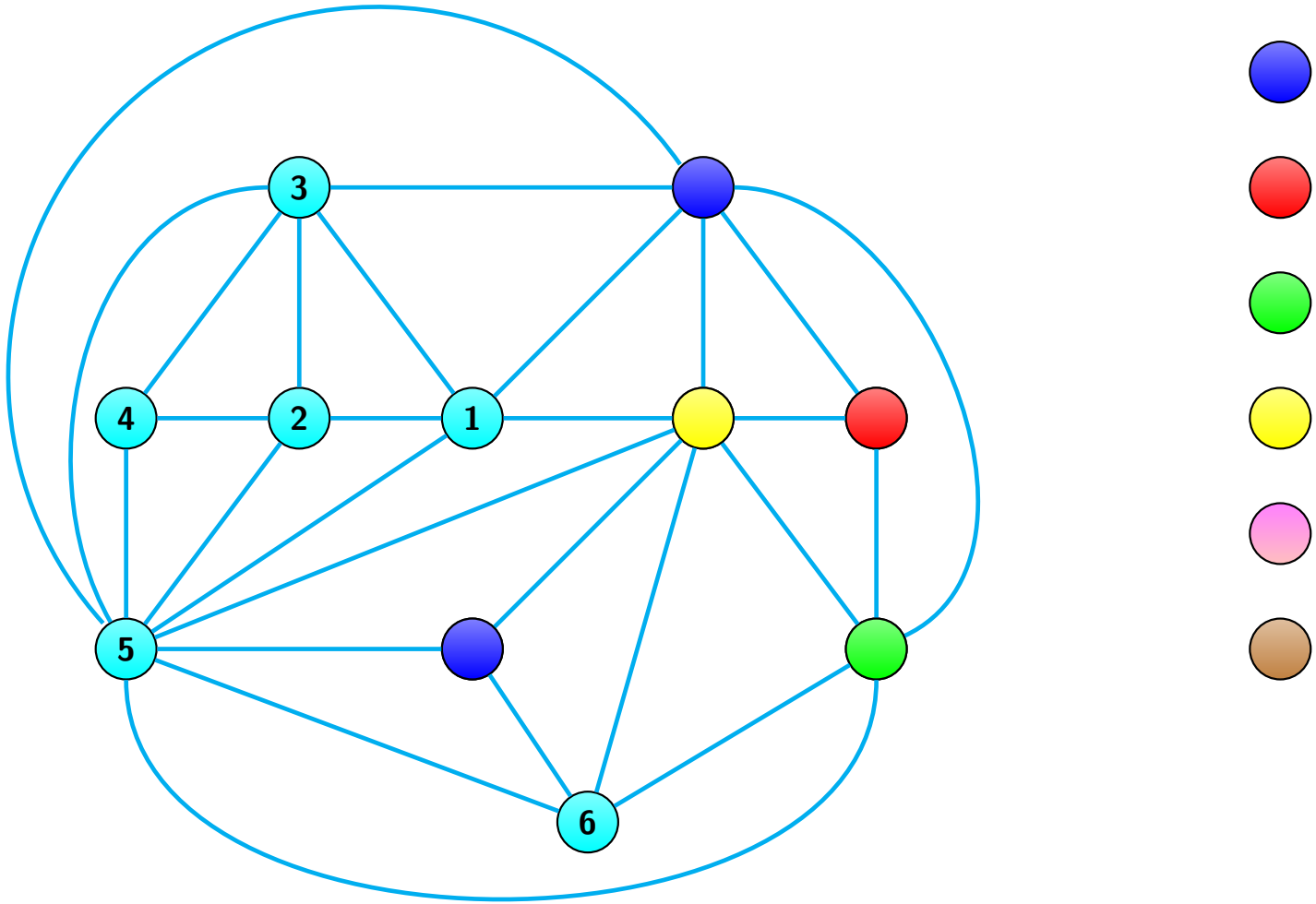
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



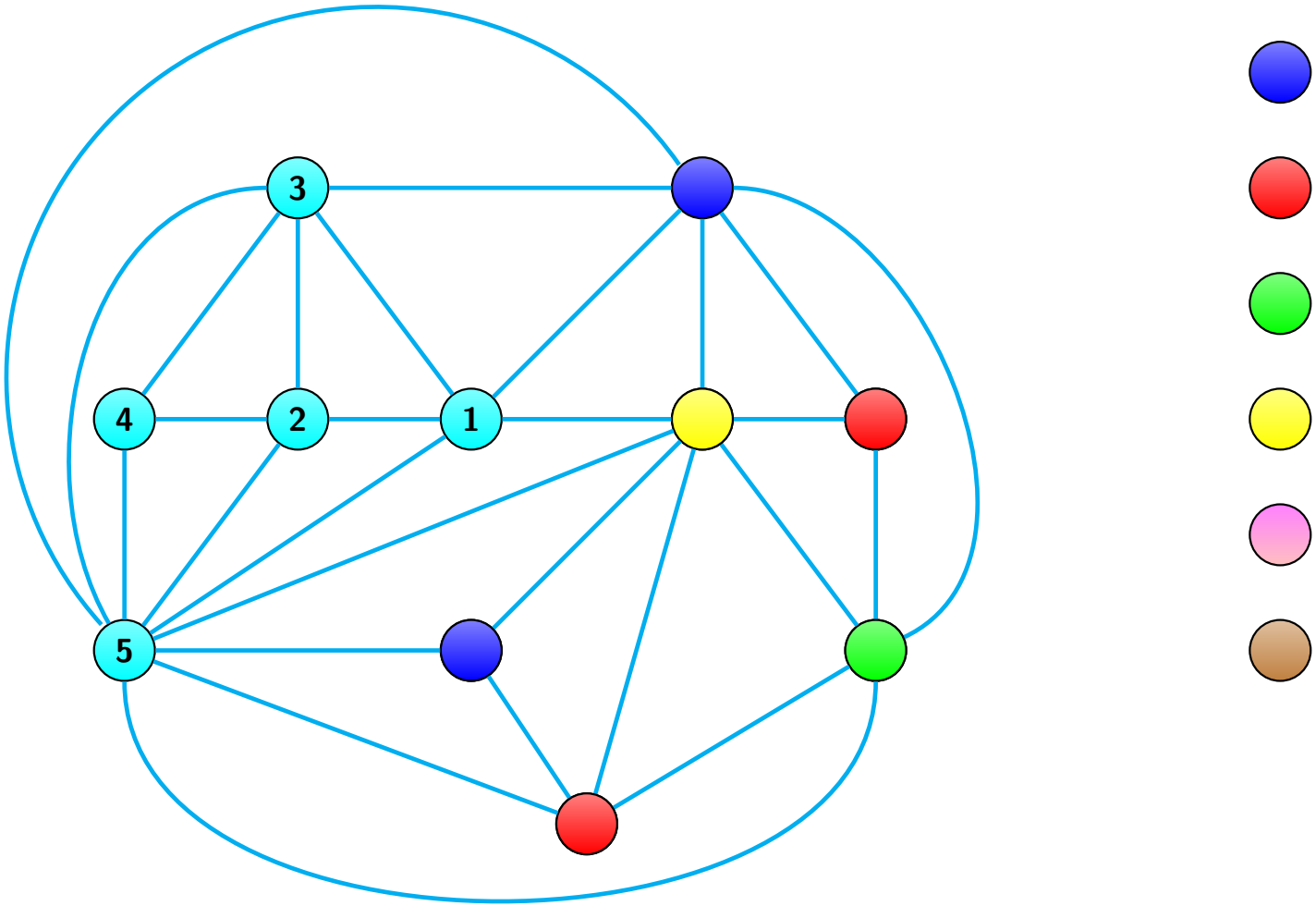
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



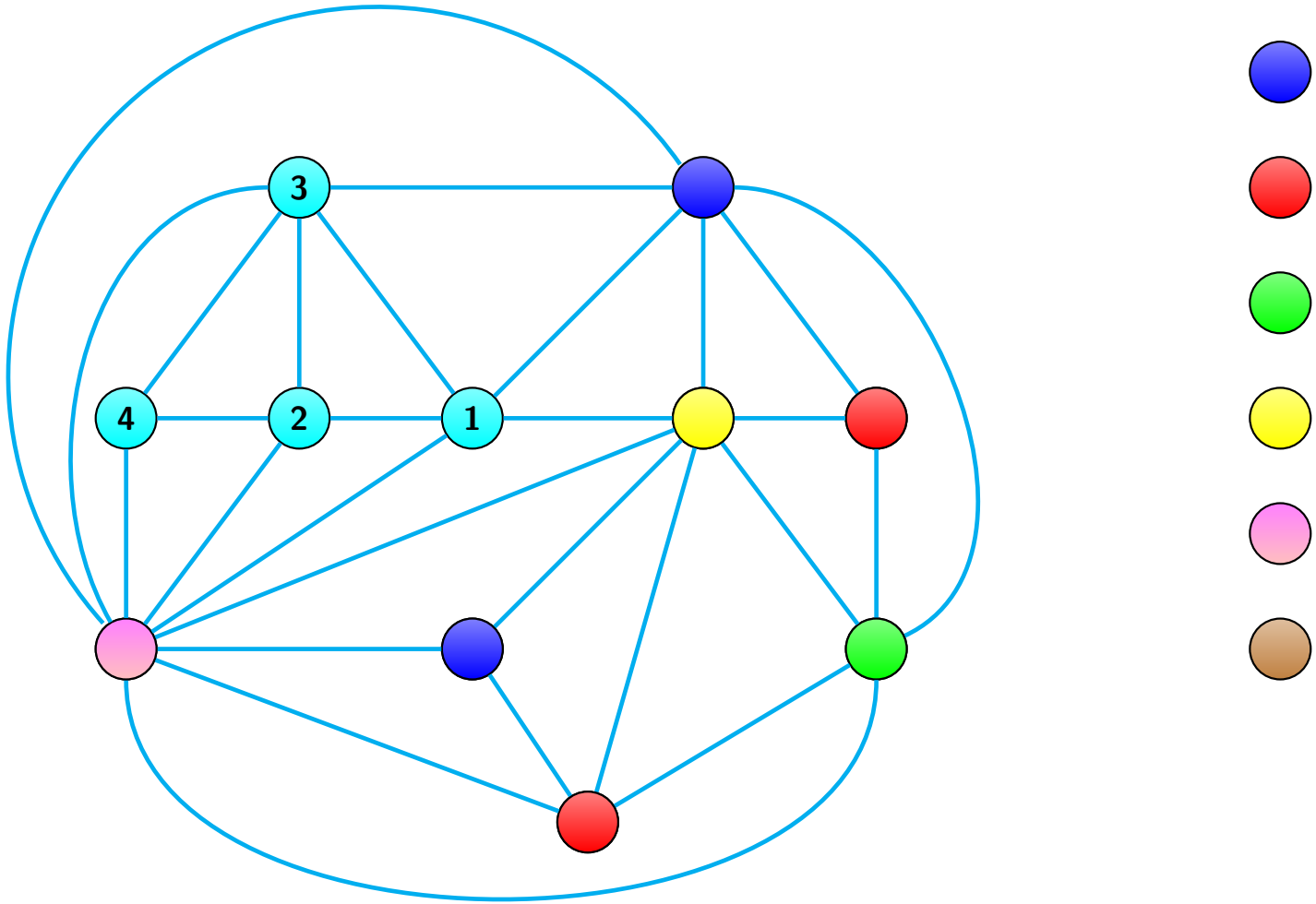
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



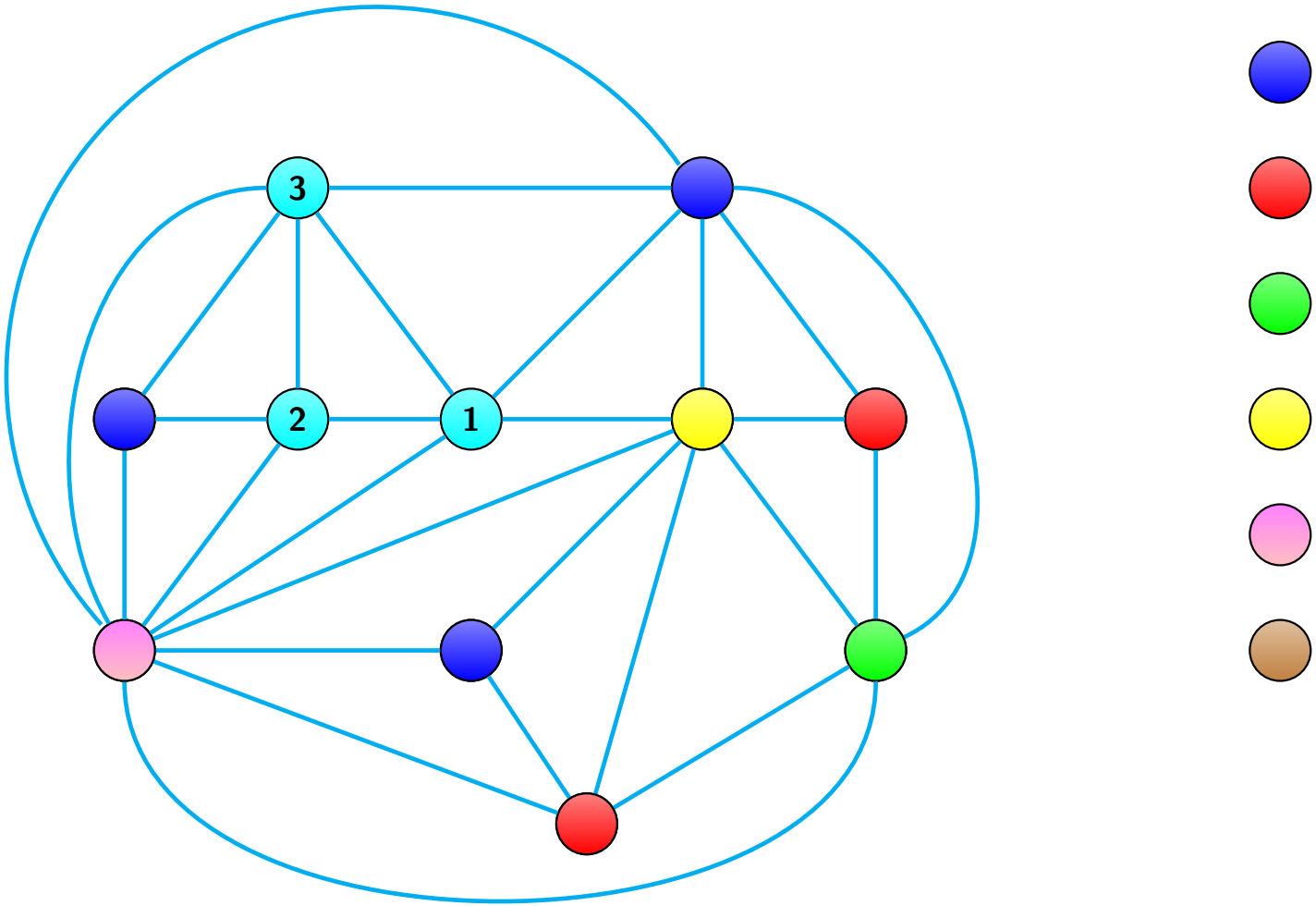
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



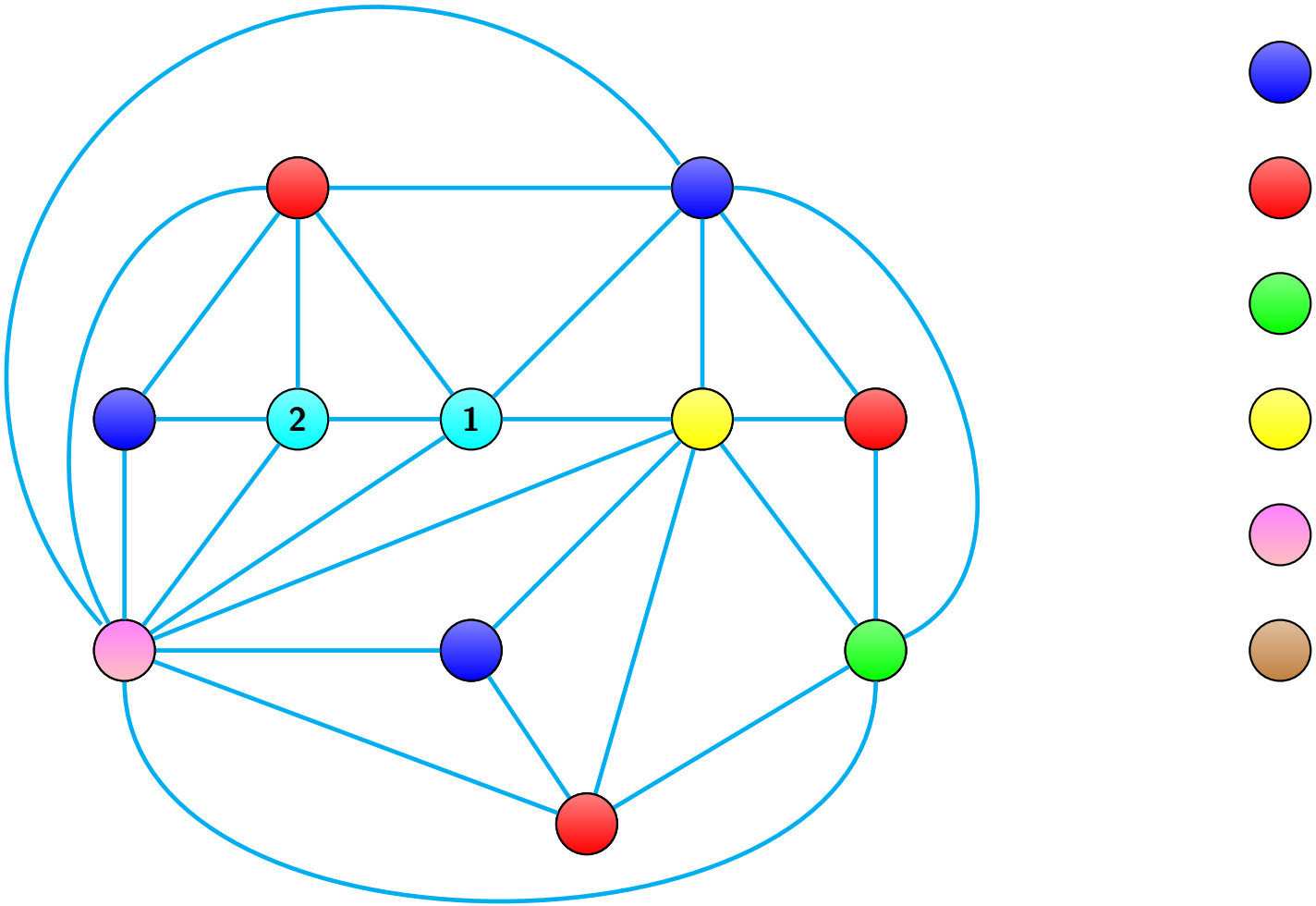
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



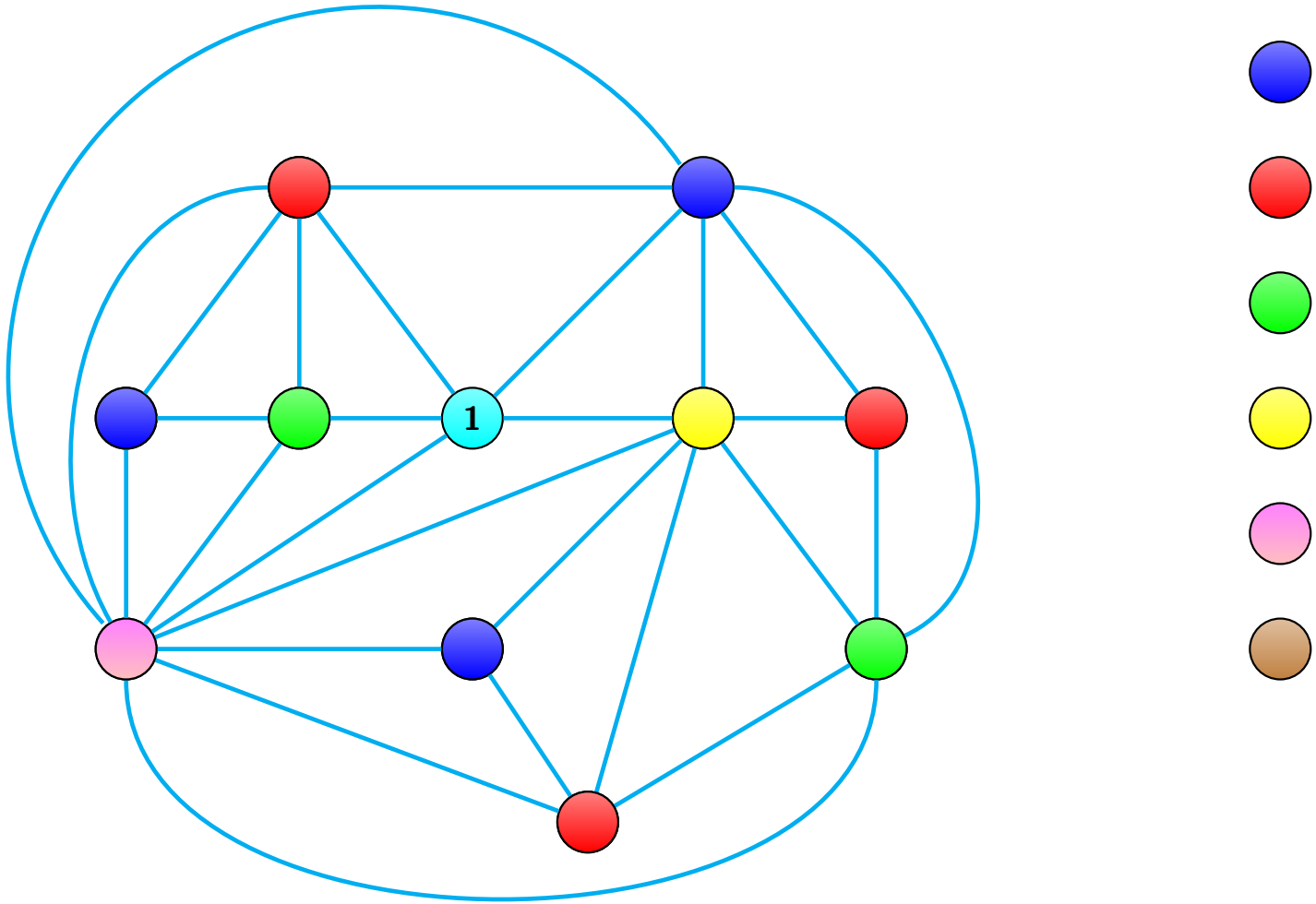
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.



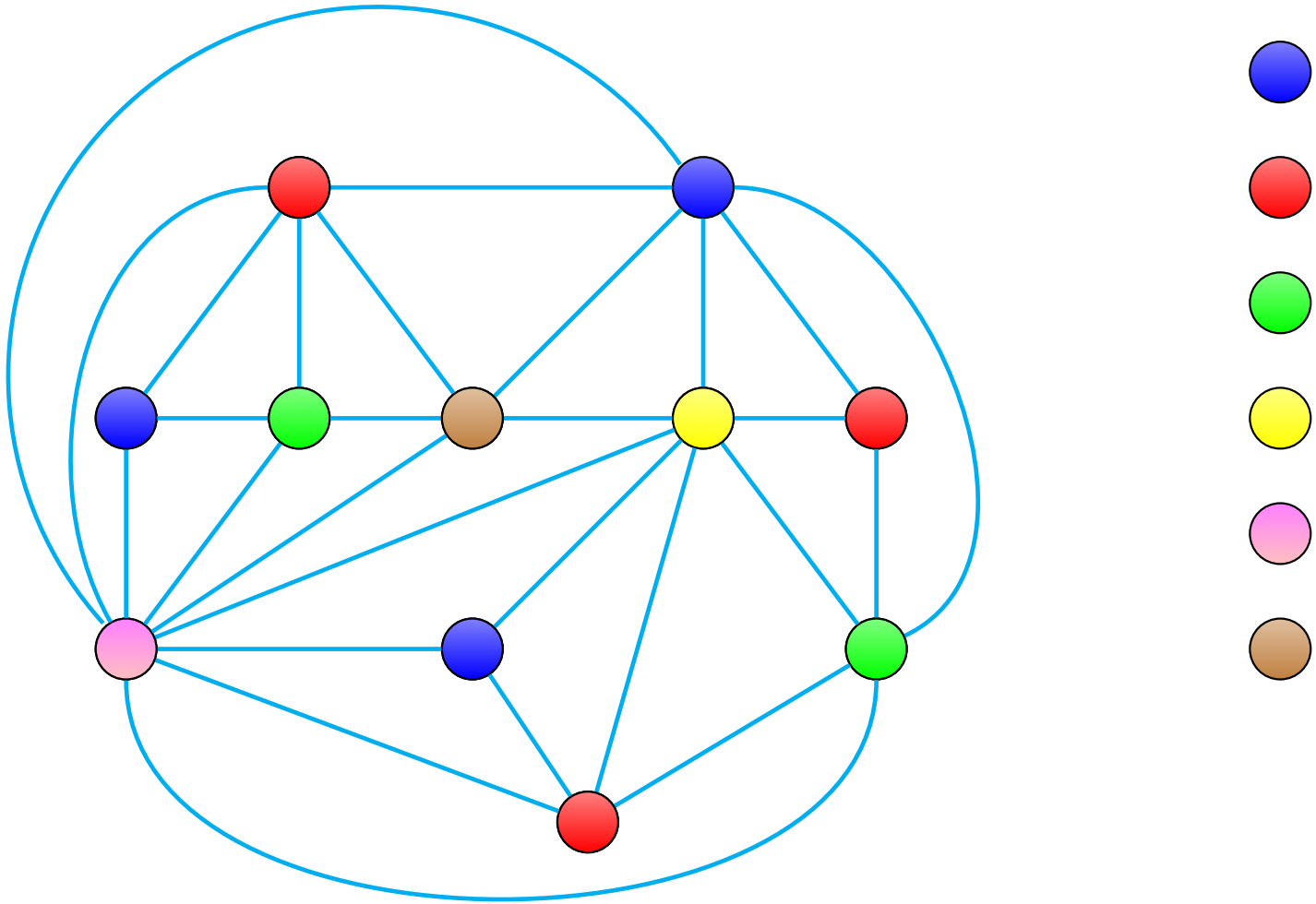
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.

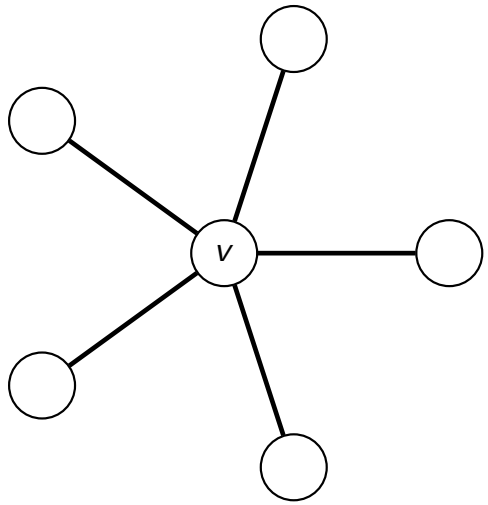


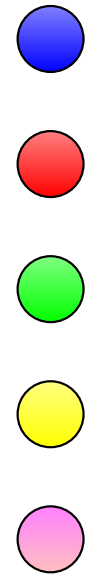
Théorème des 6 couleurs

Formule d'Euler : tout graphe planaire a un sommet adjacent à au plus 5 autres.

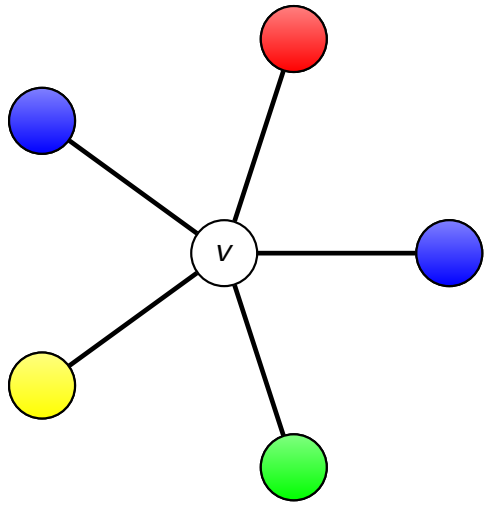


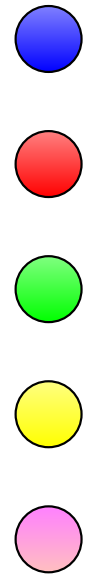
Théorème des 5 couleurs



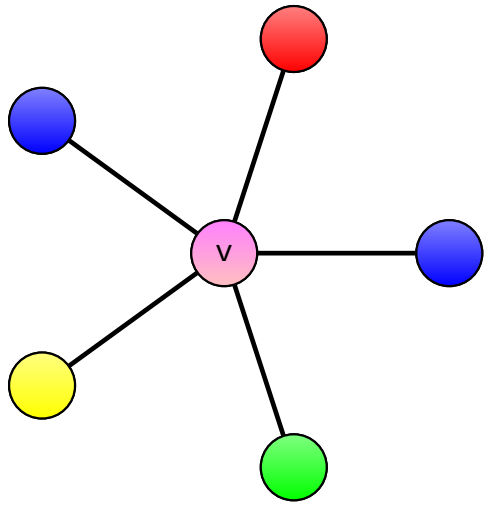


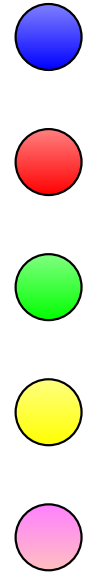
Théorème des 5 couleurs



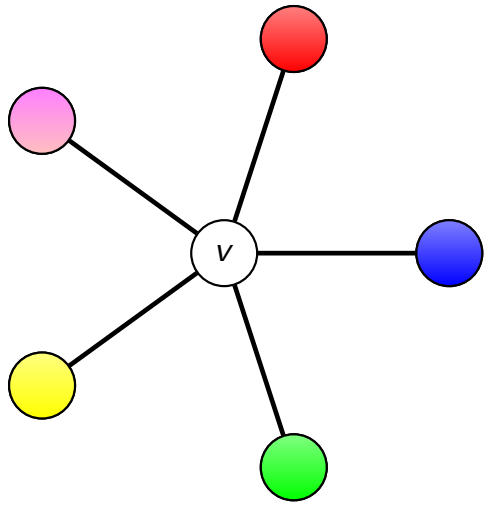


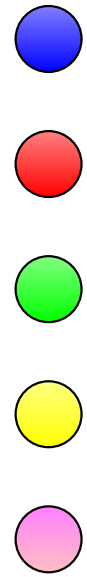
Théorème des 5 couleurs



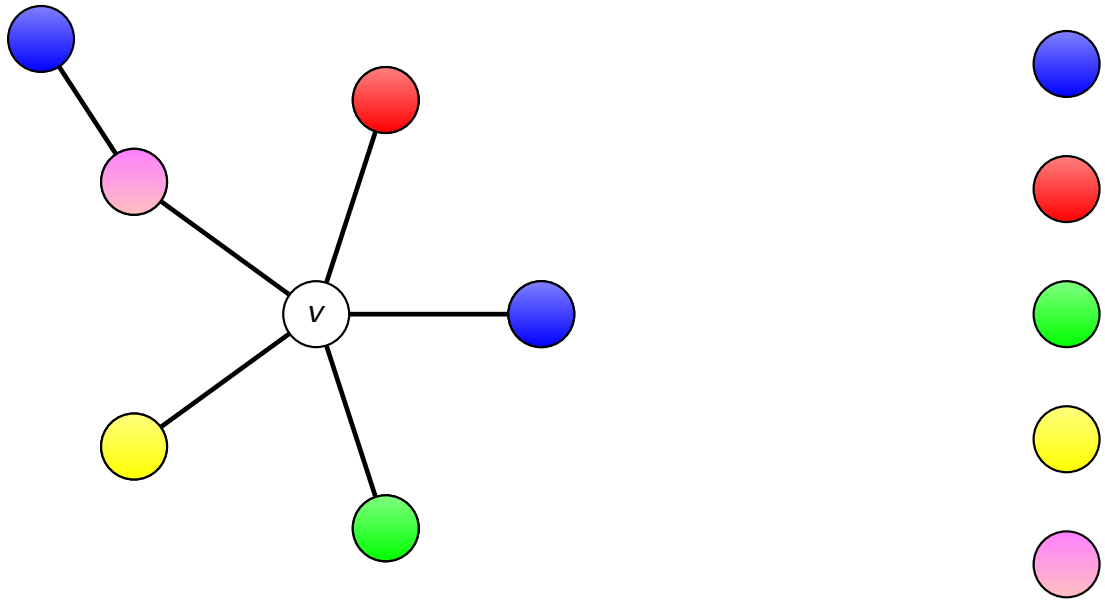


Théorème des 5 couleurs

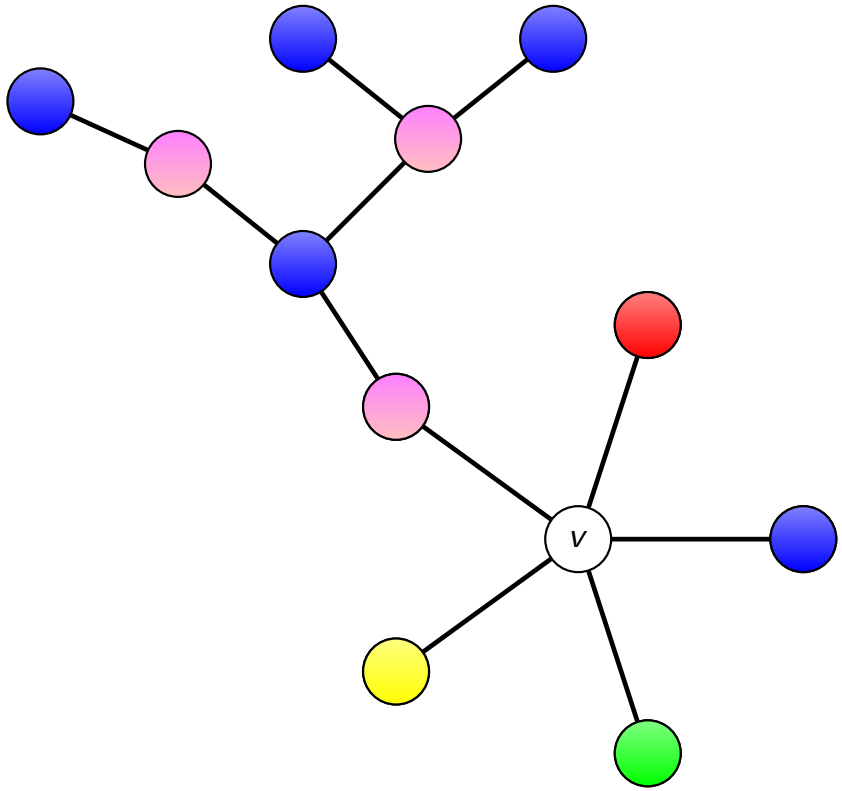




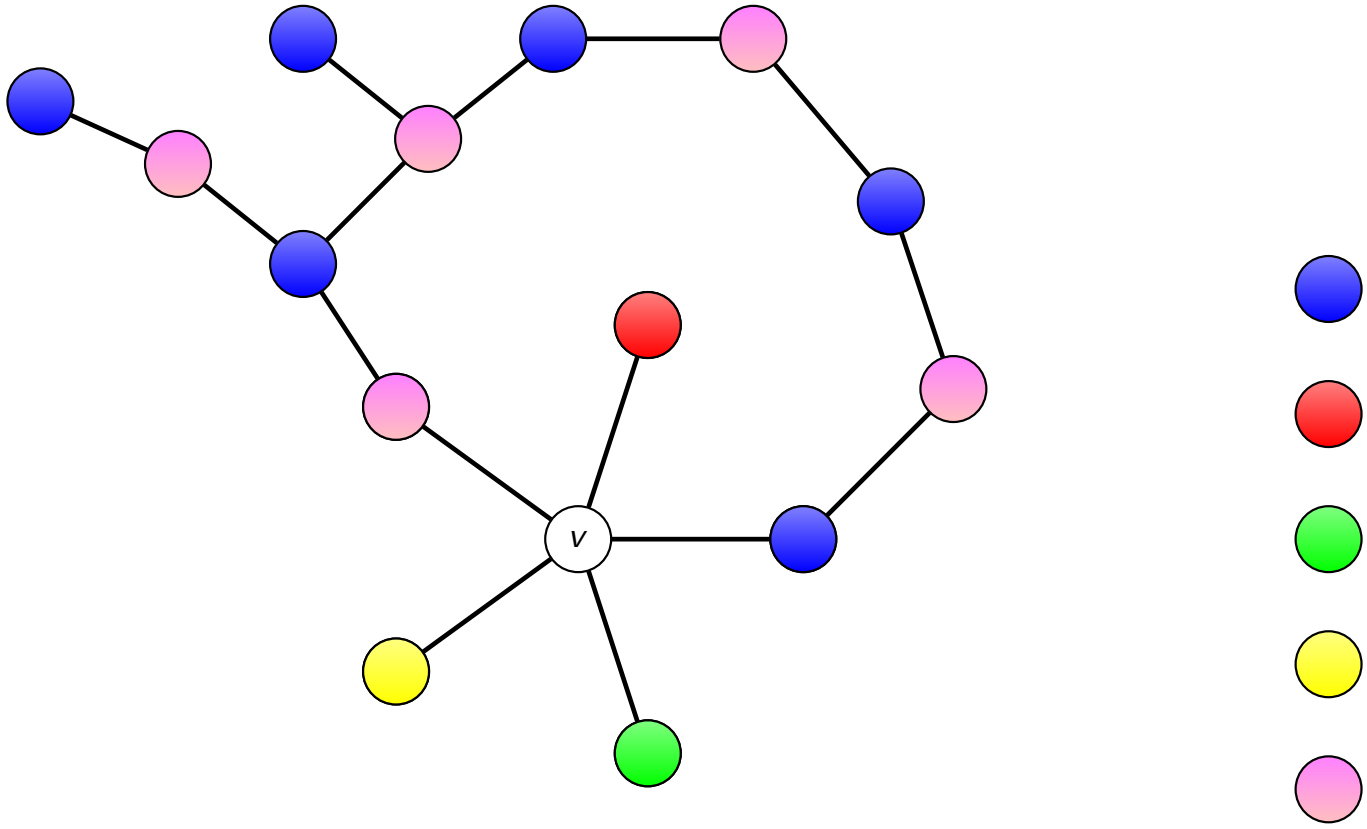
Théorème des 5 couleurs



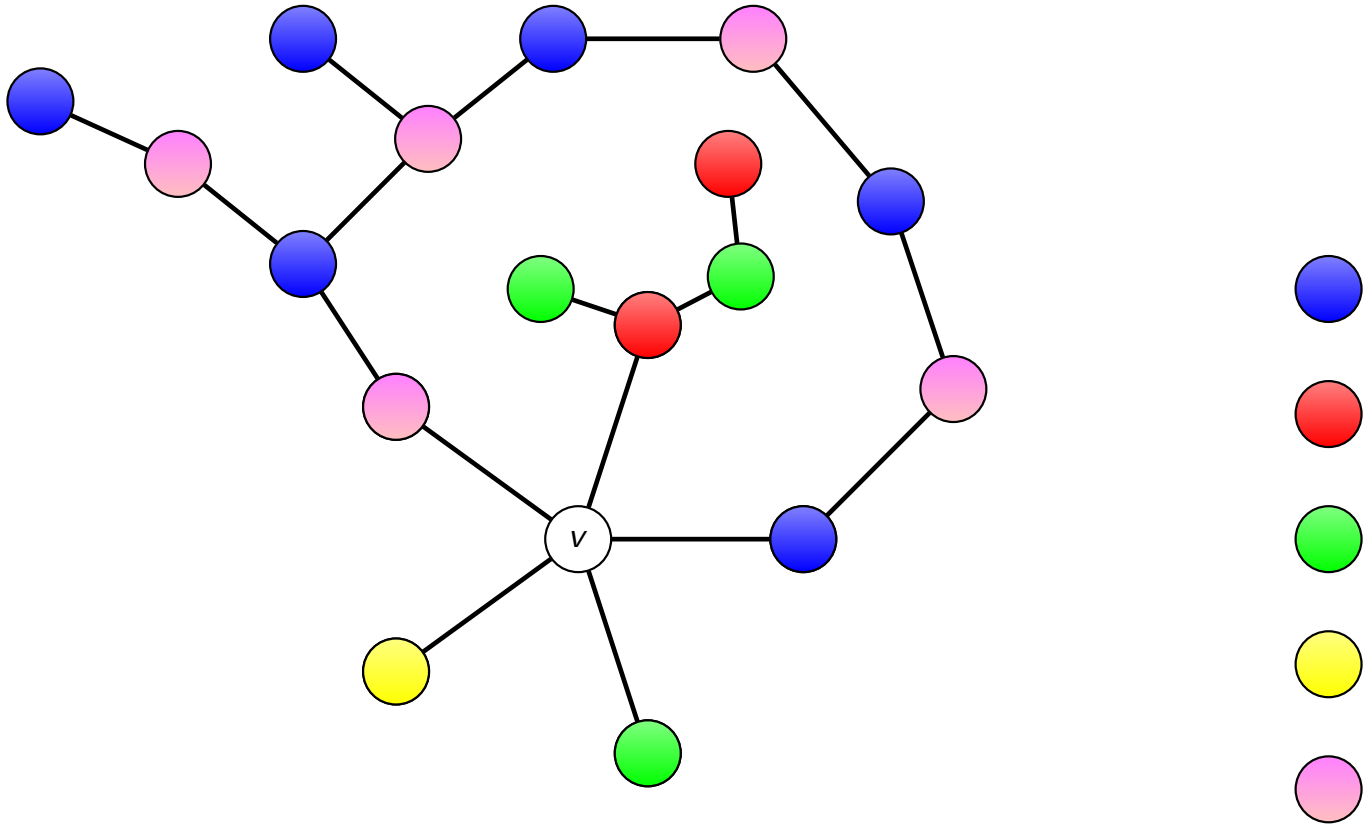
Théorème des 5 couleurs



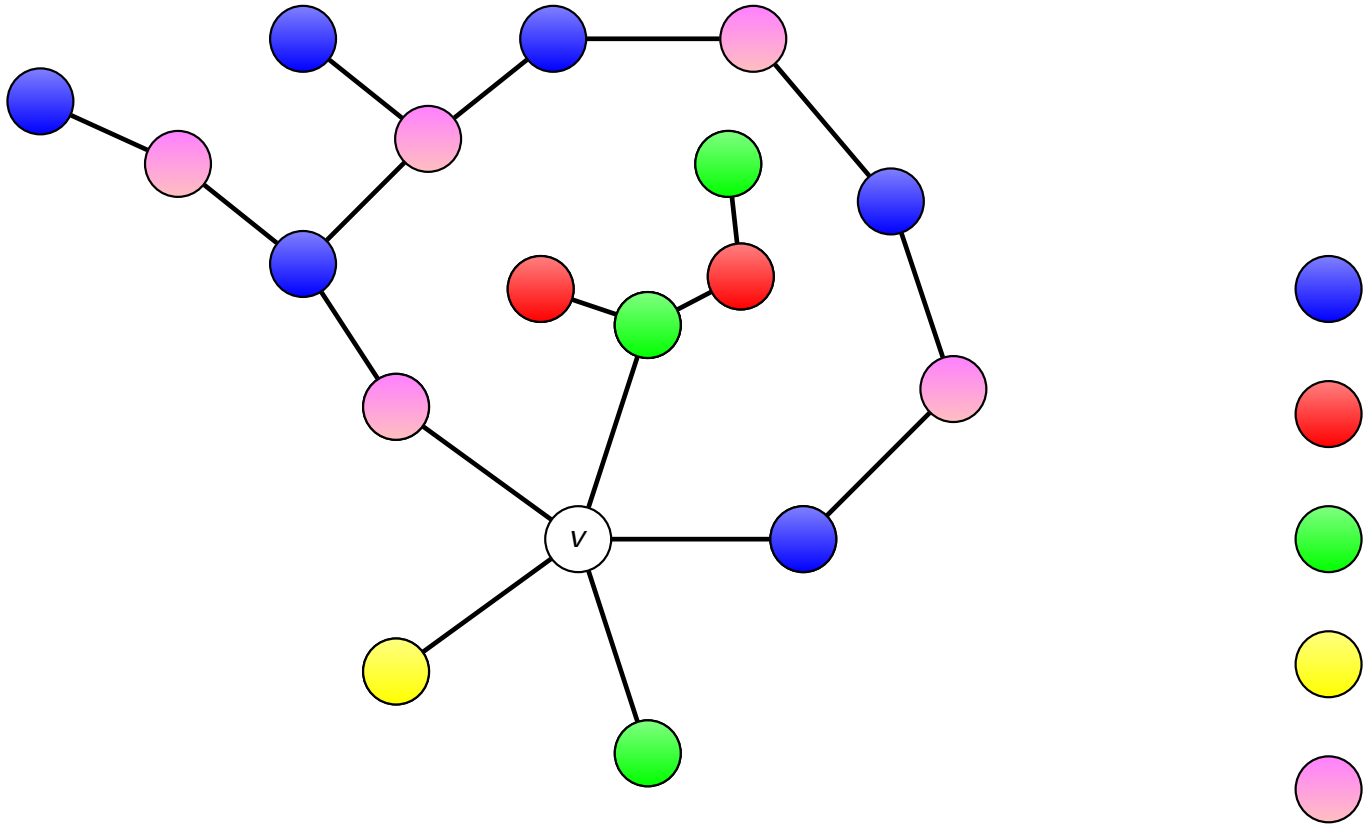
Théorème des 5 couleurs



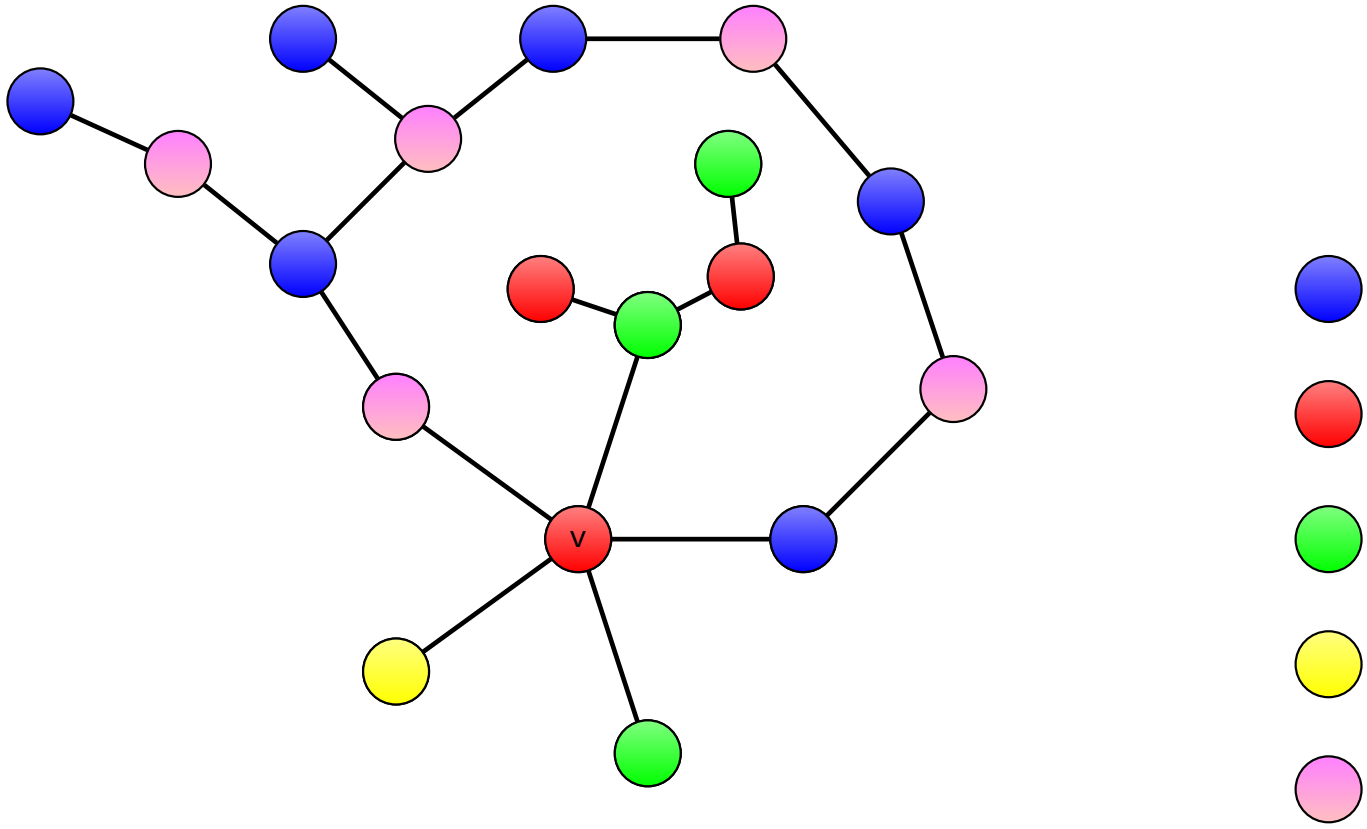
Théorème des 5 couleurs



Théorème des 5 couleurs



Théorème des 5 couleurs



Problème des 4 couleurs : les preuves

1976 : **Preuve par Kenneth Appel et Wolfgang Haken**.
Réduction à 1478 graphes.

Utilisation de l'ordinateur avec John Koch pour résoudre ces cas.

K. Appel et W. Haken
(1932 – 2013) (1928 –)

Problème pour la validation :

- Vérification de l'algorithme.
- Vérification de l'implémentation.

Problème philosophique : une "preuve" est-elle vraiment une preuve si vous ne pouvez pas la vérifier à la main ?

Problème des 4 couleurs : les preuves

1995 : **Nouvelle preuve par N. Robertson, D. Sanders, P. Seymour et R. Thomas**. Réduction à 633 cas.
Requiert toujours l'aide de l'ordinateur.

2004 : Version formalisée en Coq par G. Gonthier et B. Werner permet une vérification automatique par ordinateur.

Les 23 problèmes de Hilbert

David Hilbert
(1862 – 1943)

1. **Hypothèse du continu.**
   Indécidable (Gödel 1938, Cohen 1963).

2. **Cohérence de l'arithmétique.**
   Improuvable avec arithmétique seule. (Gödel 1931)
   Preuve avec rÃ©currence transfinie. (Grentzen, 1938)

3. **DÃ©coupage de polyÃšdres.** RÃ©solu (Dehn 1900) par la nÃ©gative.

8. **Hypothèse de Riemann.** Non résolue.

   Conjecture de Goldbach. Non résolue.
   Tout nombre pair est la somme de deux premiers.

   Conjecture des nombres premiers jumeaux. Non résolue.
   Infinité de premiers p tel que $p+2$ est premier.

Les 7 problèmes du millénaire

Le Clay Mathematical Institute : 1 million de dollars pour la résolution de chacun des problèmes suivants :

1. **Hypothèse de Riemann** (1859).
   Un des problèmes de Hilbert non résolus.
2. **Conjecture de Poincaré** (1904).
   prouvée par G. Perelman 2003.
3. **Problème P $\neq$ NP ?** ($\sim$1950).
4. **Conjecture de Hodge** ($\sim$1930).
5. **Conjecture de Birch et Swinnerton-Dyer** ($\sim$1960)
6. **Equations de Navier-Stokes** (19ème siècle).
7. **Equations de Yang-Mills** (années 1950).

Steve Smale a également proposé une liste de 17 problèmes (dont les 1,2,3,6).

Coloration de graphes : force brute

Algorithme **force brute** : tester **toutes les possibilités**.

Pour voir si un graphe à n sommets est colorable avec 4 couleurs : essayer toutes les combinaisons. On a 4 choix par sommet.
Au total, $\underbrace{4 \times 4 \times \cdots \times 4}_{n \text{ fois}} = 4^n$ possibilités.

Si $n = 135$, cela fait $4^{135} \simeq 10^{81}$ opérations.

$10^{81} \simeq$ nombre d'atomes dans l'univers.

Coloration de graphes : force brute

Algorithme **force brute** : tester **toutes les possibilités**.

Pour voir si un graphe à n sommets est colorable avec 4 couleurs : essayer toutes les combinaisons. On a 4 choix par sommet.
Au total, $\underbrace{4 \times 4 \times \cdots \times 4}_{n \text{ fois}} = 4^n$ possibilités.

Si $n = 135$, cela fait $4^{135} \simeq 10^{81}$ opérations.

$10^{81} \simeq$ nombre d'atomes dans l'univers.

On recherche des **algorithmes RAPIDES**

C'est à dire en temps polynomial (n^c opérations pour une constante c).

Le problème P ≠ NP ?

P résolubles rapidement

$+, -, \times, \div$	mariage stable	PGCD
tri	itinéraire	être premier ?

Le problème P ≠ NP ?

échecs

NP vérifiables rapidement

4-coloration sudoku voyageur de commerce

repliement de protéines ordonnancement

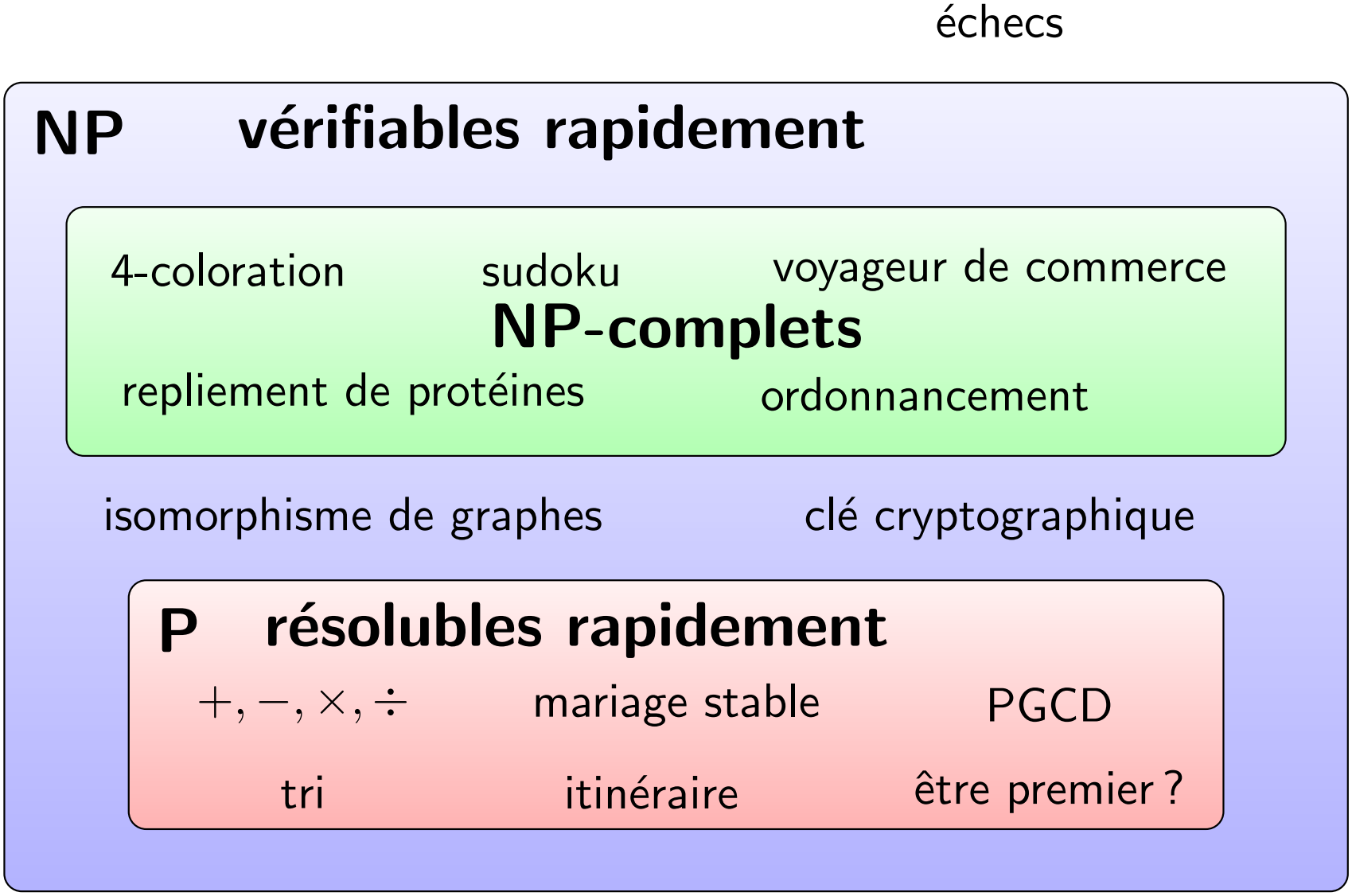
isomorphisme de graphes clé cryptographique

P résolubles rapidement

$+, -, \times, \div$ mariage stable PGCD

tri itinéraire être premier ?

Le problème P ≠ NP ?



La Conjecture de Syracuse

- Prenez un nombre entier n ;
- S'il est pair, divisez-le par 2 ; $n := 2n$;
- S'il est impair, mutipliez le par 3 et ajoutez 1 ; $n := 3n + 1$;
- Recommencez avec le résultat obtenu.

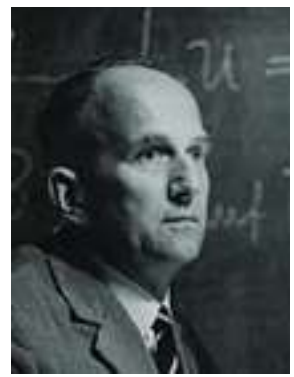
$13 \to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \cdots$

La Conjecture de Syracuse

- Prenez un nombre entier n ;
- S'il est pair, divisez-le par 2 ; $n := 2n$;
- S'il est impair, mutipliez le par 3 et ajoutez 1 ; $n := 3n + 1$;
- Recommencez avec le résultat obtenu.

$$13 \to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \cdots$$

Conjecture (Collatz 1928)
Quel que soit n,
on finit par retomber sur 1.



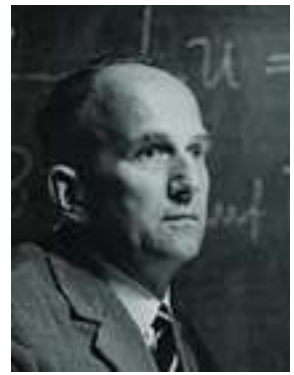
Lothar Collatz (1910 – 1990)

La Conjecture de Syracuse

- Prenez un nombre entier n ;
- S'il est pair, divisez-le par 2 ; $n := 2n$;
- S'il est impair, mutipliez le par 3 et ajoutez 1 ; $n := 3n + 1$;
- Recommencez avec le résultat obtenu.

$13 \to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1 \to 4 \cdots$

Conjecture (Collatz 1928)
Quel que soit n,
on finit par retomber sur 1.



Lothar Collatz (1910 – 1990)

vérifiée pour $n < 1,25 \times 2^{62}$. ($\sim$ 6 milliards de milliards).

≪ *Mathematicians aren't satisfied because they know there are solutions up to four million or four billion, they really want to know that there are solutions up to infinity.* ≫

Andrew Wiles