L'Univers selon Leibniz, le graphe infini aléatoire et les nombres premiers

Jean Doyen*
jdoyen@ulb.ac.be

Résumé

Les mathématiques permettent de faire des choses extraordinaires ! Le but de cet exposé est de construire et d'étudier un graphe qu'on appelle le *graphe infini aléatoire* et qui a des propriétés incroyables, défiant le bon sens.

Les ingrédients de base sont de nature arithmétique et font l'objet des trois premières sections du texte ci-dessous.

Sommaire

*Jean Doyen est Professeur au Département de Mathématique de l'Université libre de Bruxelles. Il est titulaire d'un Doctorat en Sciences Mathématiques de l'Université libre de Bruxelles. Il travaille en mathématiques discrètes et il s'est spécialisé en histoire des mathématiques.

1 Nombres premiers

La suite des nombres premiers (c'est-à-dire des nombres naturels ayant exactement deux diviseurs distincts)

$$2, 3, 5, 7, 11, 13, 17, \ldots, 97, \ldots, 23456789, \ldots, 345676543, \ldots$$

intrigue les mathématiciens depuis l'Antiquité. Au III^{e} siècle avant J.C., Euclide a prouvé le théorème fondamental suivant, dont la démonstration est un joyau d'élégance et d'inventivité :

Théorème d'Euclide. Il existe une infinité de nombres premiers.

En pratique, il est très difficile de construire explicitement de grands nombres premiers. Le plus grand connu actuellement est

$$2^{43112609} - 1$$

qui a 12 978 189 chiffres décimaux et qui a été découvert en août 2008 à UCLA (University of California in Los Angeles), avec l'aide de plus de 100 000 ordinateurs travaillant en parallèle dans le GIMPS (Great Internet Mersenne Prime Search). Les nombres premiers de la forme $2^n - 1$ (par exemple 3, 7, 31, 127) sont appelés nombres premiers de Mersenne ; actuellement, on n'en connaît que 47 mais on conjecture qu'il en existe une infinité.

Voyons comment raffiner le théorème d'Euclide en étudiant la façon dont les nombres premiers se répartissent modulo 4 :

$\equiv 0 \pmod 4$	
$\equiv 1 \pmod 4$	5 13 17 29 …
$\equiv 2 \pmod 4$	2
$\equiv 3 \pmod 4$	3 7 11 19 23 31 …

Il est clair que la première ligne de ce tableau est vide, et que la troisème comprend un seul nombre premier, à savoir 2. Qu'en est-il des deux autres lignes ? On va pouvoir prouver que chacune comprend une infinité de nombres premiers.

Théorème. *Il existe une infinité de nombres premiers* $\equiv 3 \pmod 4$.

Démonstration. Il suffit de modifier légèrement l'idée d'Euclide. Procédons par l'absurde et supposons qu'il n'y en ait qu'un nombre fini :

$$3, 7, 11, 19, 23, 31, \ldots, p_k.$$

Posons $n = 4 \cdot (3 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 31 \cdot \cdots \cdot p_k) - 1$.

Comme n est impair et plus grand que 1, tous ses facteurs premiers sont impairs. S'ils étaient tous $\equiv 1 \pmod 4$, n lui-même serait $\equiv 1 \pmod 4$. Mais n est un multiple de 4 moins 1 (par construction), autrement dit $n \equiv 3 \pmod 4$. Il existe donc un nombre premier $p \equiv 3 \pmod 4$ qui divise n. En conclusion,

$$\begin{aligned} & p \mid 4 \cdot (3 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 31 \cdot \cdots \cdot p_k) - 1 \quad \text{car } p \mid n \\ \text{et} \quad & p \mid 4 \cdot (3 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 31 \cdot \cdots \cdot p_k) \quad \text{car } p \equiv 3 \pmod 4 \end{aligned}$$

d'où on déduit que $p \mid 1$, une contradiction ! □

On démontrera dans la section 2 qu'il existe aussi une infinité de nombres premiers $\equiv 1 \pmod 4$.

Remarque. Le tableau ci-dessus pourrait laisser croire que les nombres premiers $\equiv 3 \pmod 4$ sont un peu plus nombreux que ceux qui sont $\equiv 1 \pmod 4$, car il semble qu'il y en a toujours plus dans la quatrième ligne que dans le deuxième. En fait, lorsqu'on arrivera à 26861, il y en aura plus dans la ligne des $\equiv 1 \pmod 4$. On peut démontrer que les nombres premiers sont répartis avec la même densité dans ces deux lignes.

Le théorème suivant, conjecturé par Legendre en 1785 et démontré par Dirichlet en 1837, généralise le cas particulier que nous venons de prouver. On n'en connaît aucune démonstration « élémentaire » : la démonstration classique nécessite notamment l'utilisation des fonctions de variable complexe et des représentations de groupes ; on la trouvera par exemple dans le remarquable « Cours d'arithmétique » de Jean-Pierre Serre [1].

Théorème de Dirichlet. Si a et m sont des entiers strictement positifs tels que $\operatorname{pgcd}(a, m) = 1$, il existe une infinité de nombres premiers $\equiv a \pmod m$.

Autrement dit, si $\operatorname{pgcd}(a, m) = 1$, la suite arithmétique

$$a, a + m, a + 2m, a + 3m, \ldots$$

contient une infinité de nombres premiers. Il est facile de voir que l'hypothèse $\operatorname{pgcd}(a, m) = 1$ est indispensable pour arriver à cette conclusion.

Voici une conséquence immédiate du théorème de Dirichlet :

Corollaire. *Il existe une infinité de nombres premiers dont les n derniers chiffres en système décimal sont fixés, à condition bien entendu que le dernier chiffre soit* 1, 3, 7 *ou* 9.

Démonstration. Notons $b_1, b_2, b_3, \ldots, b_n$ les n derniers chiffres, avec $b_j \in \{0, 1, 2, \ldots, 9\}$ et $b_n = 1, 3, 7$ ou 9. Il suffit de remarquer que

$$\operatorname{pgcd}(b_1 b_2 b_3 \ldots b_n, 10^n) = 1$$

où $b_1 b_2 b_3 \ldots b_n$ représente le nombre naturel dont l'écriture en système décimal se compose des chiffres successifs $b_1, b_2, b_3, \ldots, b_n$. □

Ce résultat a été amélioré en 1959 par le mathématicien polonais Wacław Sierpiński [2] :

Théorème de Sierpiński. Il existe une infinité de nombres premiers

$$p = a_1 a_2 \ldots a_m \ldots b_1 b_2 \ldots b_n$$

dont les m premiers chiffres et les n derniers (en système décimal) sont fixés, avec $a_i, b_j \in \{0, 1, 2, \ldots, 9\}$, $a_1 \neq 0$, $b_n = 1, 3, 7$ ou 9.

Question 1. Existe-t-il des suites arithmétiques dont tous les termes sont des nombres premiers ?

Il est très facile de prouver que la réponse est NON : il suffit de remarquer que pour tout entier $n \geqslant 2$, les $n-1$ entiers consécutifs

$$n!+2, n!+3, \ldots, n!+n$$

sont tous non premiers. L'ensemble $\mathbb{N}$ des nombres naturels contient donc des intervalles de longueur arbitrairement grande dépourvus de nombres premiers, et toute suite arithmétique aura donc au moins un de ses termes dans un de ces intervalles.

Question 2. Existe-t-il des progressions arithmétiques de longueur arbitrairement grande, dont tous les termes sont des nombres premiers ?

Ce problème est beaucoup plus difficile. Voici quelques exemples :

1. $3, 5, 7$ (longueur 3)
2. $5, 11, 17, 23, 29$ (longueur 5)
3. $43142746595714191 + k \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 23681770$, pour $k = 0, \ldots, 25$ (longueur 26 ; découverte en avril 2010, c'est la plus longue connue explicitement à l'heure actuelle).

En 2004, Ben Green et Terence Tao [3] (ce dernier a reçu une médaille Fields en 2006) ont réussi à démontrer que la réponse à la question 2 est OUI ! De plus, ils ont prouvé qu'il existe une telle progression de longueur L dont tous les termes sont plus petits que

$$2^{2^{2^{2^{2^{2^{100L}}}}}}.$$

Un peu d'histoire. Peter Gustav Lejeune-Dirichlet est d'origine « belge ». Ses grands-parents vivaient à Richelette, un hameau près de Liège, à quelques kilomètres à l'est de Herstal. Son père, receveur des postes, partit s'installer à Düren (entre Aachen et Köln) où le jeune Peter Gustav naquit en 1805. Sur place, on les appelait familièrement « la famille de Richelette » et le jeune fils devint donc tout naturellement « le jeune de Richelette », ce qui, prononcé à l'allemande, donnera « Lejeune-Dirichlet ».

Dirichlet était un grand admirateur de Gauß. On raconte que les « Disquisitiones Arithmeticae », génial traité d'arithmétique publié par Gauß en 1801, ne le quittaient jamais et qu'il dormait même avec ce livre sous son oreiller. En plus de ses travaux en théorie des nombres, Dirichlet apporta des contributions fondamentales en analyse (convergence des séries de Fourier, analyse harmonique, théorie du potentiel) et en combinatoire (applications du principe des tiroirs de Dirichlet).

Professeur à Breslau puis à Berlin, il succéda à Gauß à Göttingen en 1855. Après sa mort en 1859, son cerveau fut conservé dans le Département de physiologie de l'Université de Göttingen.

2 Carrés dans $\mathbb{Z}_p$

Lorsque p est un nombre premier, on sait que l'ensemble $\mathbb{Z}_p \overset{\text{def}}{=} \{0, 1, \ldots, p-1\}$ des entiers modulo p est un corps. L'ensemble des éléments non nuls de $\mathbb{Z}_p$, noté $\mathbb{Z}_p^*$, est un groupe multiplicatif d'ordre $p-1$.

Considérons par exemple $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$. En élevant chacun de ses éléments au carré (ce qui est plus rapide en écrivant $4 = -3$, $5 = -2$ et $6 = -1$), on trouve $0,1,4,2$. On dira que les carrés de $\mathbb{Z}_7$ sont $1,2,4$ (0 n'est pas considéré comme un carré) et les non-carrés $3,5,6$.

Plus généralement, si p est un nombre premier *impair*, le corps $\mathbb{Z}_p$ comprend exactement $\frac{p-1}{2}$ carrés et $\frac{p-1}{2}$ non-carrés. Pour le montrer, il suffit de remarquer que l'application

$$\alpha : \mathbb{Z}_p^* \to \mathbb{Z}_p^* : x \mapsto x^2$$

est un morphisme de groupes multiplicatifs, dont le noyau, constitué des $x \in \mathbb{Z}_p^*$ tels que $x^2 = 1$, est formé des deux éléments 1 et -1 (comme p est impair, on a bien $1 \neq -1$).

Il est clair que 1 est toujours un carré de $\mathbb{Z}_p$. Qu'en est-il de -1 ?

Théorème. *Si -1 est un carré dans $\mathbb{Z}_p$ (p premier impair), alors* $p \equiv 1 \pmod 4$.

Démonstration. Par hypothèse, il existe un $x \in \mathbb{Z}_p^*$ tel que $x^2 = -1$. Comme $x^4 = 1$ et que $x^2 \neq 1$ (car $-1 \neq 1$), on en déduit que x est d'ordre 4 dans le groupe multiplicatif $\mathbb{Z}_p^*$ d'ordre $p-1$. Par le théorème de Lagrange, on a donc $4 \mid p-1$, c'est-à-dire $p \equiv 1 \pmod 4$. □

En fait, la réciproque est vraie : -1 est un carré dans $\mathbb{Z}_p$ si et seulement si $p \equiv 1 \pmod 4$, mais nous ne le démontrerons pas ici.

Corollaire. *Il existe une infinité de nombres premiers* $\equiv 1 \pmod 4$.

Démonstration. Supposons (pour rire, puisque ce n'est pas vrai !) qu'il n'y en ait qu'un nombre fini

$$5, 13, 17, 29, \ldots, p_k$$

Posons $n = (2 \cdot 5 \cdot 13 \cdot 17 \cdot 29 \cdot \ldots \cdot p_k)^2 + 1$. Comme n est impair et strictement plus grand que 1, il existe un diviseur premier impair p de n. On a donc

$$(2 \cdot 5 \cdot 13 \cdot 17 \cdot 29 \cdot \ldots \cdot p_k)^2 + 1 \equiv 0 \pmod p$$

c'est-à-dire $(2 \cdot 5 \cdot 13 \cdot 17 \cdot 29 \cdot \ldots \cdot p_k)^2 \equiv -1 \pmod p$, d'où il résulte que -1 est un carré dans $\mathbb{Z}_p$, donc que $p \equiv 1 \pmod 4$ par le théorème précédent. Autrement dit, p est un des nombres premiers $5, 13, 17, 29, \ldots, p_k$. En conclusion, $p \mid n$ et $p \mid n-1$, d'où on déduit que $p \mid 1$, une contradiction. □

Symbole de Legendre. Puisque les carrés de $\mathbb{Z}_p$ (avec p premier impair) forment un sous-groupe d'indice 2 du groupe multiplicatif $\mathbb{Z}_p^*$, les carrés (□) et non-carrés (⊠) de $\mathbb{Z}_p$ se comportent multiplicativement comme dans la table ci-dessous

·	□	⊠
□	□	⊠
⊠	⊠	□

qui est analogue à

·	1	−1
1	1	−1
−1	−1	1

Ceci donne l'idée d'introduire, pour tout $a \in \mathbb{Z}_p$, le symbole $\left(\frac{a}{p}\right)$ (qui se lit « a sur p » et qui est appelé *symbole de Legendre*) défini par

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a = \square \\ -1 & \text{si } a = \not\square \\ 0 & \text{si } a = 0 \end{cases}$$

Il découle de ce qu'on vient de voir que

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \qquad \forall a, b \in \mathbb{Z}_p$$

Le symbole de Legendre, qui est au départ défini dans $\mathbb{Z}_p$, peut être étendu à $\mathbb{Z}$ en posant

$$\left(\frac{a}{p}\right) \stackrel{\text{def}}{=} \left(\frac{a \bmod p}{p}\right) \qquad \forall a \in \mathbb{Z}$$

Par exemple, $\left(\frac{23}{7}\right) = \left(\frac{2}{7}\right) = 1$, $\left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1$, et $\left(\frac{14}{7}\right) = \left(\frac{0}{7}\right) = 0$. On voit facilement que le symbole de Legendre étendu à $\mathbb{Z}$ jouit toujours de la propriété de multiplicativité

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \qquad \forall a, b \in \mathbb{Z}.$$

Le résultat fondamental suivant, conjecturé par Euler et Legendre, a été démontré par Gauß en 1796. Il avait 19 ans et il écrit : « Pendant toute une année, ce théorème m'a tourmenté et a absorbé tous mes efforts, jusqu'à ce que j'en obtienne une démonstration. » Par après, Gauß en a donné 8 démonstrations différentes ; actuellement, on en connaît plus de 150 (voir par exemple Murray Gerstenhaber [4]).

Loi de réciprocité quadratique de Gauß. Si p et q sont des nombres premiers impairs distincts, alors

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

sauf si $p \equiv q \equiv 3 \pmod 4$, auquel cas

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Notons qu'on peut formuler cet énoncé de manière équivalente mais plus compacte comme suit (exercice) :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Il y a bien une « réciprocité » dans cette loi : si p est un carré modulo q, alors réciproquement q est un carré modulo p (sauf si $p \equiv q \equiv 3 \pmod 4$).

Voici deux exemples très simples montrant comment on peut appliquer en pratique la loi de Gauß :

1. On calcule successivement

$$\left(\frac{19}{43}\right) = -\left(\frac{43}{19}\right) = -\left(\frac{5}{19}\right) = -\left(\frac{19}{5}\right) = -\left(\frac{4}{5}\right) = -1,$$

donc 19 n'est pas un carré dans $\mathbb{Z}_{43}$.

2. De même,

$$\left(\frac{15}{43}\right) = \left(\frac{3\cdot 5}{43}\right) = \left(\frac{3}{43}\right)\left(\frac{5}{43}\right) = -\left(\frac{43}{3}\right)\left(\frac{43}{5}\right) = -\left(\frac{1}{3}\right)\left(\frac{3}{5}\right) = -\left(\frac{5}{3}\right) = -\left(\frac{2}{3}\right) = 1,$$

donc 15 est un carré dans $\mathbb{Z}_{43}$.

Pour mieux apprécier la puissance de la loi de Gauß, résolvons le problème non-trivial suivant : dans quels corps $\mathbb{Z}_p$ (p premier strictement plus grand que 3) 3 est-il un carré ?

D'une part

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{si } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{3}\right) & \text{si } p \equiv 3 \pmod 4 \end{cases}$$

D'autre part

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 & \text{si } p \equiv 1 \pmod 3 \\ \left(\frac{2}{3}\right) = -1 & \text{si } p \equiv 2 \pmod 3 \end{cases}$$

Par conséquent

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{si } \begin{cases} p \equiv 1 \pmod 4 \text{ et } p \equiv 1 \pmod 3 \\ \text{ou} \\ p \equiv 3 \pmod 4 \text{ et } p \equiv 2 \pmod 3 \end{cases} \\ -1 & \text{si } \begin{cases} p \equiv 1 \pmod 4 \text{ et } p \equiv 2 \pmod 3 \\ \text{ou} \\ p \equiv 3 \pmod 4 \text{ et } p \equiv 1 \pmod 3 \end{cases} \end{cases}$$

Autrement dit

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{ssi } p \equiv \pm 1 \pmod{12} \\ -1 & \text{ssi } p \equiv \pm 5 \pmod{12} \end{cases}$$

Conclusion : 3 est un carré dans $\mathbb{Z}_p$ (p premier strictement plus grand que 3) si et seulement si $p = \pm 1 \pmod{12}$.

Exercice. Dans quels corps $\mathbb{Z}_p$ le nombre 5 est-il un carré ? (pour p premier strictement plus grand que 5.)

Un peu d'histoire. Adrien-Marie Legendre (Paris 1752, Paris 1833) est l'auteur de nombreux travaux mathématiques : en théorie des nombres (symbole de Legendre, preuve de l'irrationalité de π^2), en géométrie (réécriture des *Elements* d'Euclide), en analyse (polynômes de Legendre, équation différentielle de Legendre, traité des fonctions elliptiques et des intégrales eulériennes).

Il ne faut pas le confondre avec Louis Legendre (Versaille 1752 ou 1755 ou 1756 ? ; Paris 1797) qui n'a aucun lien de parenté avec le mathématicien. Louis Legendre fut d'abord marin pendant 10 ans, puis ouvrit une boucherie à Saint-Germain-des-Prés à Paris. Très actif pendant la Révolution française, il participa à la prise de la Bastille et devint député de la Montagne à l'Assemblée législative (les « Montagnards » étaient les députés siégeant sur les bancs les plus hauts de l'Assemblée) où il vota la mort de Louis XVI. Souffrant de démence à la fin de sa vie, il fut toutefois encore élu au Conseil des 500.

En 2005, deux étudiants de l'Université de Strasbourg s'étaient étonnés de retrouver partout le même portrait pour les deux hommes : la lithographie censée représenter Adrien-Marie Legendre dans tous les livres de mathématiques était-elle celle du mathématicien ou celle du politicien ? La réponse se trouvait dans l'ouvrage « Iconographie des contemporains depuis 1789 jusqu'en 1829 », publié en 1833 et contenant notamment les portraits des députés Montagnards : il s'agissait bien du politicien ! Dès lors, où trouver un portrait du mathématicien ? En 2008, on découvre dans la Bibliothèque de l'Institut de France un « Album de 73 portraits-charge aquarellés des membres de l'Institut » (en fait des caricatures assez féroces mais très ressemblantes, faites par un certain Boilly) : une caricature du mathématicien Legendre y apparaît à côté de celle de Fourier ! (pour y accéder, aller sur le site `http://www.photo.rmn.fr`, cliquer sur Recherche, puis taper `Boilly`).

Une dernière remarque : le nom du politicien était Legendre (en un seul mot), tandis que le mathématicien signait Le Gendre (en deux mots).

3 Lemme chinois

Dans les « Disquisitiones Arithmeticae » de Gauß (1801), on trouve une démonstration du résultat suivant :

Lemme chinois (ou *Chinese remainder theorem*). Si $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ sont des entiers et si $m_1, m_2, \ldots, m_k$ sont des entiers strictement positifs tels que $\operatorname{pgcd}(m_i, m_j) = 1$ pour tout $i \neq j$, alors le système de congruences

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

a au moins une solution $x \in \mathbb{Z}$. De plus, cette solution est unique modulo $m_1 \cdot m_2 \cdot \cdots \cdot m_k$.

Remarques. 1. L'hypothèse $\operatorname{pgcd}(m_i, m_j) = 1$ pour tout $i \neq j$ est indispensable : par exemple, le système

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 1 \pmod{6} \end{cases}$$

n'a aucune solution $x \in \mathbb{Z}$ puisque x doit être pair d'après la première congruence et impair d'après la deuxième.

2. Pourquoi l'adjectif « chinois » ? Parce que dans un livre d'arithmétique de Sun-Tsŭ (1^{er} siècle après J.C.), on trouve des problèmes du type : trouver un entier n qui, après division par 3, 5, 7, donne respectivement pour restes 2, 3, 2. Autrement dit, trouver n tel que

$$\begin{cases} n \equiv 2 \pmod 3 \\ n \equiv 3 \pmod 5 \\ n \equiv 2 \pmod 7. \end{cases}$$

Le lemme chinois affirme qu'un tel entier existe et qu'il est unique modulo $3 \cdot 5 \cdot 7 = 105$. Vérifions-le explicitement :

- $n \equiv 2 \pmod 3$ implique qu'il existe $t \in \mathbb{Z}$ tel que $n = 3t + 2$.
- De $n = 3t + 2 \equiv 3 \pmod 5$, on déduit successivement :
  $\Longrightarrow \quad 3t \equiv 1 \pmod 5$
  $\Longrightarrow \quad t \equiv 2 \pmod 5$
  $\Longrightarrow \quad \exists t' \in \mathbb{Z}$ tel que $t = 5t' + 2$
  $\Longrightarrow \quad n = 3(5t' + 2) + 2 = 15t' + 8$
- De $n = 15t' + 8 \equiv 2 \pmod 7$, on déduit alors :
  $\Longrightarrow \quad t' \equiv 1 \pmod 7$
  $\Longrightarrow \quad \exists t'' \in \mathbb{Z}$ tel que $t' = 7t'' + 1$
  $\Longrightarrow \quad n = 15(7t'' + 1) + 8 = 105t'' + 23$

Les solutions du système sont donc tous les entiers $n \equiv 23 \pmod{105}$.

4 L'Univers selon Leibniz

Gottfried Wilhelm Leibniz (Leipzig 1646, Hannover 1716) est, avec Newton, un des pères fondateurs du calcul infinitésimal. Son œuvre est immense et, à ce jour, personne n'a entrepris d'en faire l'édition complète (il a laissé plus de 200 000 feuilles manuscrites). Ses écrits philosophiques n'ont pas toujours été bien compris : dans « Candide » en 1759, Voltaire se moque de Leibniz sous les traits du docteur Pangloss, qui répète sans cesse, au milieu des pires catastrophes, que « Tout va pour le mieux dans le meilleur des mondes possibles ! »

Laissons la parole à Leibniz, qui écrit notamment : « Comme il y a une infinité d'univers possibles dans les idées de Dieu et qu'il n'en peut exister qu'un seul, il faut qu'il y ait une raison suffisante du choix de Dieu, qui le détermine à l'un plutôt qu'à l'autre. » En 1697 Leibniz publie « De rerum originatione radicale » (Sur les principes fondamentaux à l'origine des choses) où il formule diverses hypothèses métaphysiques sur notre univers, hypothèses qui peuvent se résumer comme suit :

1. Le monde réel est le meilleur de tous les mondes possibles. Plus précisément, le monde réel maximise d'une part son degré de symétrie (sa « beauté ») et d'autre part la variété de ses sous-structures.
2. Le meilleur des mondes possibles est la structure aléatoire la plus probable.

On va construire maintenant un objet mathématique très simple vérifiant ces deux hypothèses (et d'autres auxquelles Leibniz n'avait sans doute pas pensé).

Auparavant, pour détendre l'atmosphère, voici une citation d'Hubert Curien, physicien français qui fut ministre de la recherche sous François Mitterrand :

« S'il se présentait comme chercheur au CNRS, Dieu serait refusé. Il a fait une manipulation intéressante, mais jamais personne n'a pu la reproduire. Il a expliqué ses travaux dans une grosse publication, il y a très longtemps, mais ce n'était même pas en anglais et, depuis, il n'a plus rien publié. »

5 Le graphe infini aléatoire

Dans ce qui suit, $\aleph_0$ désigne comme d'habitude le plus petit cardinal infini, c'est-à-dire l'infini dénombrable.

Étant donné un ensemble S de cardinal $\aleph_0$, on peut construire un graphe ayant pour sommets les éléments de S en procédant comme suit : pour chaque paire $\{p, q\}$ d'éléments de S, on lance une pièce de monnaie parfaitement symétrique (probabilité de pile égale à 1/2) pour décider si oui ou non p et q sont joints par une arête, les jets étant supposés indépendants. On dira que le graphe Γ ainsi obtenu est un graphe infini aléatoire, car sa construction dépend du hasard.

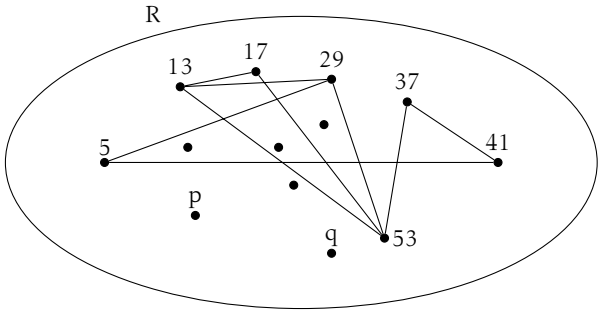
On va maintenant définir un graphe R ayant lui aussi $\aleph_0$ sommets, mais dont la construction est tout à fait déterministe. Les sommets de R sont les nombres premiers $\equiv 1 \pmod 4$; par le théorème de Dirichlet, R a donc $\aleph_0$ sommets. Un sommet p est relié par une arête à un autre sommet q (ce qu'on notera $p \sim q$) si et seulement si p est un carré modulo q, autrement dit

$$p \sim q \iff \left(\frac{p}{q}\right) = 1$$

Par la loi de réciprocité quadratique de Gauß,

$$p \equiv q \equiv 1 \pmod 4 \qquad \Longrightarrow \qquad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

autrement dit $p \sim q \Rightarrow q \sim p$. Le graphe R ainsi construit est donc non-dirigé : les arêtes sont des paires (et non des couples) de sommets. Voici quelques-unes des arêtes de R :



Maintenant, un miracle se produit ! En 1963, les deux mathématiciens hongrois Paul Erdös et Alfred Rényi [5] ont démontré que la probabilité qu'un graphe infini aléatoire Γ soit isomorphe au graphe R est égale à 1 !

Théorème d'Erdös et Rényi. $\mathbb{P}(\Gamma \simeq \mathrm{R}) = 1$

En d'autres termes, en lançant une pièce de monnaie pour construire un graphe infini aléatoire, il est stochastiquement certain qu'on obtiendra le graphe R. C'est pourquoi R est appelé *le* graphe infini aléatoire (en anglais : *the* countable random graph). La lettre R est l'initiale de « random », mais aussi du prénom et du nom de Richard Rado [6] qui, en 1964, a donné une autre construction du graphe R.

Mais les miracles continuent ! En effet, R jouit de toute une série de propriétés surprenantes. En voici quelques-unes :

1. R est *indestructible* : si on partitionne l'ensemble des sommets de R en un nombre fini n de morceaux, le sous-graphe induit sur au moins un des morceaux est isomorphe à R (rappelons que, si S′ est un sous-ensemble de l'ensemble S des sommets d'un graphe G, le sous-graphe $\langle S' \rangle$ induit par G sur S′ est le graphe ayant pour sommets les éléments de S′ et pour arêtes les arêtes de G contenues dans S′). On peut prouver que les seuls graphes infinis dénombrables ayant cette propriété sont le graphe complet $K_{\aleph_0}$, son complément et le graphe R.
2. Si on ajoute ou si on enlève un nombre fini d'arêtes à R (sans modifier l'ensemble des sommets), le graphe obtenu est isomorphe à R.
3. R est *universel* : tout graphe fini ou infini dénombrable apparaît dans R comme sous-graphe induit.
4. R a énormément de symétries : si Aut R désigne son groupe d'automorphismes,
$$|\mathrm{Aut}\, R| = 2^{\aleph_0}$$
5. Aut R est un groupe *simple*, c'est-à-dire n'ayant aucun sous-groupe normal non-trivial.
6. R est *ultrahomogène*, autrement dit R jouit de la propriété de « libre mobilité » : tout isomorphisme entre deux sous-graphes induits finis de R est réalisable par un automorphisme de R (ceci sera expliqué plus en détail dans la section 6).

Le lecteur qui a gardé à l'esprit les hypothèses métaphysiques de Leibniz sur l'Univers aura compris que le graphe R constitue bel et bien un modèle d'un tel Univers. Einstein disait que « Dieu ne joue pas aux dés ». Il est tentant d'ajouter : *Non, mais il joue peut-être à pile ou face !*

Remarques. 1. On peut démontrer (voir par exemple Cameron [7, Chapitre 5]) que R est le seul graphe infini dénombrable ayant à la fois les propriétés 3 et 6 (universalité et ultrahomogénéité).

2. Si on construit un graphe aléatoire sur un nombre fini n de sommets, les graphes qui apparaîtront avec la plus petite probabilité seront ceux qui ont le plus de symétries. Par exemple, la probabilité d'obtenir le graphe complet K_n (qui a le nombre maximum d'automorphismes, à savoir $n!$) vaut $1/2^{\binom{n}{2}}$.
   En fait, on prouve facilement que la probabilité d'obtenir un graphe donné G de n sommets (à un isomorphisme près) est inversement proportionelle au nombre d'automorphismes de G. Les graphes aléatoires les plus probables sur un nombre fini de sommets seront donc les graphes rigides, c'est-à-dire ceux n'ayant pas d'autre automorphisme que l'identité. Par contre, comme on l'a dit plus haut, si on travaille avec une infinité dénombrable de sommets, la situation change du tout au tout : il est stochastiquement certain que le graphe obtenu aura énormément de symétries !

Démonstration du théorème d'Erdös et Rényi. On dira qu'un graphe G a la propriété $(*)$ si et seulement si, quels que soient les ensembles *finis* disjoints U et V de sommets de G, il existe un sommet z de G tel que $z \sim u$ pour tout $u \in U$ et $z \nsim v$ pour tout $v \in V$. Notons déjà qu'aucun graphe fini n'a la propriété $(*)$: pour s'en convaincre, il suffit de prendre pour U l'ensemble de tous les sommets de G et pour V l'ensemble vide.

Le théorème d'Erdös et Rényi découle immédiatement des trois lemmes suivants :

Lemme 1. *La probabilité qu'un graphe infini aléatoire* Γ *ait la propriété* $(*)$ *est égale à* 1.

Lemme 2. *Le graphe* R *a la propriété* $(*)$.

Lemme 3. *Deux graphes de* $\aleph_0$ *sommets ayant la propriété* $(*)$ *sont nécessairement isomorphes.*

Démonstration du lemme 1. Il faut prouver que l'événement « Γ n'a pas la propriété $(*)$ » a une probabilité nulle. Cet événement est la réunion de tous les événements « Γ n'a pas la propriété $(*)(U,V)$ », où $(*)(U,V)$ désigne la propriété $(*)$ pour un couple (U,V) *donné* d'ensembles finis disjoints de sommets de Γ. Comme il y a $\aleph_0$ tels couples (U,V) dans Γ (car Γ a $\aleph_0$ sommets) et que toute réunion dénombrable d'ensembles de mesure nulle est de mesure nulle, il suffit de prouver que l'événement « Γ n'a pas la propriété $(*)(U,V)$ » a une probabilité nulle.

Posons $k = |U \cup V|$ et notons $z_1, z_2, \ldots, z_n, \ldots$ les sommets de Γ extérieurs à $U \cup V$. On dira qu'un sommet z_i est bon s'il est adjacent (joint par une arête) à tous les $u \in U$ et non-adjacent à tous les $v \in V$; sinon on dira que z_i est mauvais. La probablité que z_i soit mauvais vaut $1 - (1/2)^k$. Par l'hypothèse d'indépendance des jets, la probabilité que les n premiers sommets $z_1, \ldots, z_n$ soient tous mauvais vaut donc

$$\left(1 - \left(\frac{1}{2}\right)^k\right)^n.$$

Comme cette expression tend vers 0 lorsque n tend vers l'infini, la probabilité que tous les z_i soient mauvais est nulle. On a donc bien prouvé que la probabilité de l'événement « Γ n'a pas la propriété $(*)(U,V)$ » est nulle. □

Remarque. Si la pièce de monnaie lancée pour construire Γ n'est pas parfaitement symétrique, c'est-à-dire si $0 < \mathbb{P}(\text{pile}) < 1$, il est facile d'adapter le raisonnement ci-dessus pour montrer que le lemme 1 reste valable, donc aussi le théorème d'Erdös-Rényi puisque les aspects probabilistes n'interviennent pas du tout dans les démonstrations des lemmes 2 et 3. Autrement dit, si on utilise par exemple une pièce de monnaie telle que $\mathbb{P}(\text{pile}) = 0{,}999\,999\,9$ et $\mathbb{P}(\text{face}) = 0{,}000\,000\,1$, le graphe aléatoire Γ obtenu sera encore isomorphe à R avec une probabilité égale à 1 !

Démonstration du lemme 2. Soient $U = \{p_1, \ldots, p_m\}$ et $V = \{q_1, \ldots, q_n\}$ deux ensembles disjoints de nombres premiers $\equiv 1 \pmod 4$. Pour tout $i = 1, \ldots, m$, choisissons un entier a_i tel que $\left(\frac{a_i}{p_i}\right) = 1$ et, pour tout $j = 1, \ldots, n$, un entier b_j tel que

$\left(\frac{b_j}{q_j}\right) = -1$. Par le lemme chinois, le système de congruences

$$\left\{\begin{array}{ll} x \equiv 1 & (\text{mod } 4) \\ x \equiv a_1 & (\text{mod } p_1) \\ \quad\vdots & \\ x \equiv a_m & (\text{mod } p_m) \\ x \equiv b_1 & (\text{mod } q_1) \\ \quad\vdots & \\ x \equiv b_n & (\text{mod } q_n) \end{array}\right. \tag{1}$$

a une solution unique

$$x \equiv x_0 \pmod{4p_1 \dots p_m q_1 \dots q_n}. \tag{2}$$

Comme $\text{pgcd}(x_0, 4p_1 \dots p_m q_1 \dots q_n) = 1$ (car x_0 n'est congru à 0 ni modulo 2, ni modulo p_i, ni modulo q_j puisque x_0 est solution du système (1)), le théorème de Dirichlet permet d'affirmer qu'il existe un nombre premier p solution de la congruence (2), donc aussi du système de congruences (1). Dès lors,

$$\begin{array}{rl} p \equiv 1 \pmod 4 & \Longrightarrow\ p \text{ est un sommet du graphe R} \\ p \equiv a_i \pmod{p_i} & \Longrightarrow\ p \sim p_i \in \mathrm{U} \\ p \equiv b_j \pmod{q_j} & \Longrightarrow\ p \nsim q_j \in \mathrm{V} \end{array}$$

On a donc bien montré que R a la propriété (∗). □

Démonstration du lemme 3. Si Γ_1 et Γ_2 sont deux graphes de $\aleph_0$ sommets ayant la propriété (∗), on veut prouver que $\Gamma_1 \simeq \Gamma_2$. Le raisonnement qui suit est dû à Peter Cameron [7] :

Soit S_1 (resp. S_2) un ensemble fini de sommets de Γ_1 (resp. de Γ_2). Supposons qu'il existe un isomorphisme α du sous-graphe induit $\langle \mathrm{S}_1 \rangle$ sur le sous-graphe induit $\langle \mathrm{S}_2 \rangle$. Alors, si z_1 est un sommet quelconque de Γ_1 n'appartenant pas à S_1, on peut étendre α à $\mathrm{S}_1 \cup \{z_1\}$. En effet, soit U_1 (resp. V_1) l'ensemble des sommets de S_1 adjacents (resp. non-adjacents) à z_1 dans le graphe Γ_1. Posons $\mathrm{U}_2 = \alpha(\mathrm{U}_1)$ et $\mathrm{V}_2 = \alpha(\mathrm{V}_1)$. Comme Γ_2 a la propriété (∗), il existe un sommet z_2 de Γ_2 qui est adjacent à tous les sommets de U_2 et non-adjacent à tous les sommets de V_2. Il suffit de poser $\alpha(z_1) = z_2$ pour étendre l'isomorphisme de $\langle \mathrm{S}_1 \rangle$ sur $\langle \mathrm{S}_2 \rangle$ en un isomorphisme α' de $\langle \mathrm{S}_1 \cup \{z_1\} \rangle$ sur $\langle \mathrm{S}_2 \cup \{z_2\} \rangle$.

Numérotons $a_1, a_2, \dots$ les sommets de Γ_1 et $b_1, b_2, \dots$ ceux de Γ_2.

Étape numéro 1. On part de $\mathrm{S}_1 = \{a_1\}$ et $\mathrm{S}_2 = \{b_1\}$. Il existe clairement un isomorphisme $\alpha_1 : \langle \mathrm{S}_1 \rangle \to \langle \mathrm{S}_2 \rangle$.

Étape numéro 2. On étend α_1 à $\mathrm{S}_1 \cup \{a_2\}$ et on obtient ainsi un isomorphisme $\alpha_2 : \langle \{a_1, a_2\} \rangle \to \langle \{b_1, b_j\} \rangle$ pour un certain $j > 1$.

Si on continuait de la même manière en étendant α_2 en α_3 et ainsi de suite, on obtiendrait évidemment une injection de Γ_1 dans Γ_2 à la fin du processus, mais on ne serait pas certain que ce soit une bijection ! L'astuce consiste à procéder comme suit à l'étape numéro n :

Si n est impair, on prend comme sommet z_1 le sommet de Γ_1 ayant le plus petit indice et n'appartenant pas au domaine de α_{n-1}, et on étend α_{n-1} en α_n.

Si n est pair, on prend comme sommet z_2 le sommet de Γ_2 ayant le plus petit indice et n'appartenant pas à l'image de α_{n-1}, et on étend α_{n-1}^{-1} en α_n^{-1} (c'est-à-dire aussi α_{n-1} en α_n).

Après une infinité dénombrable d'étapes, tous les sommets de Γ_1 seront dans le domaine de α et tous les sommets de Γ_2 seront dans l'image de α, donc on aura une bijection $\alpha : \Gamma_1 \to \Gamma_2$ qui sera, par construction, un isomorphisme de Γ_1 sur Γ_2. □

Remarque. En s'inspirant du raisonnement développé ci-dessus, il est facile de démontrer que le graphe R a les propriétés 3 et 6 d'universalité et d'ultrahomogénéité.

6 Homogénéité et ultrahomogénéité

Soit S un ensemble muni d'une structure (graphe, ensemble ordonné, espace métrique, etc.) On dit que S est *homogène* si, chaque fois que les structures induites sur deux sous-ensembles *finis* S_1 et S_2 de S sont isomorphes, il existe un automorphisme de S appliquant S_1 sur S_2. On dit que S est *ultrahomogène* si *tout* isomorphisme de S_1 sur S_2 s'étend en un automorphisme de S.

Il est clair que S ultrahomogène implique S homogène.

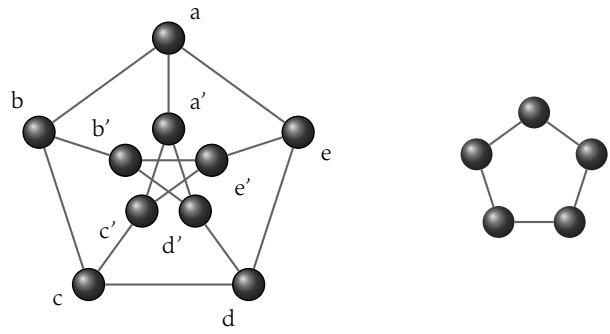


FIGURE 1 — Le graphe de Petersen (à gauche) et le graphe du pentagone (à droite).

Exemples. 1. Le graphe de Petersen (voir figure 1) n'est pas homogène car, malgré que les sous-graphes induits sur les ensembles de sommets $S_1 = \{a', b, e\}$ et $S_2 = \{b', c', d\}$ soient isomorphes, il n'existe pas d'automorphisme de S appliquant S_1 sur S_2 : en effet, les sommets a', b, e ont un sommet adjacent commun (à savoir a), ce qui n'est pas le cas pour b', c', d ;

2. Le graphe du pentagone est homogène, et même ultrahomogène ;
3. Le graphe de l'hexagone n'est ni l'un ni l'autre (exercice facile).

Il est clair que le complément de tout graphe homogène (resp. ultrahomogène) est aussi homogène (resp. ultrahomogène).

On prouve facilement que tout graphe non-connexe (fini ou infini) homogène est réunion disjointe de graphes complets isomorphes (exercice).

Théorème (Sheehan [8] 1974, Gardiner [9] 1976, Gol'fand et Klin [10] 1978). *Les graphes finis ultrahomogènes sont*

1. *les réunions disjointes de graphes complets isomorphes finis,*
2. *les compléments des précédents,*
3. *le graphe du pentagone,*
4. *la grille* 3×3 *:*

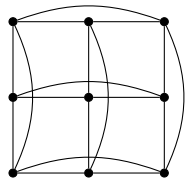


FIGURE 2 — *La grille* 3×3.

Théorème (Ronse [11] 1978). *La liste des graphes finis homogènes est exactement la même.*

Les graphes infinis dénombrables ultrahomogènes ont été classés en 1980 par Lachlan et Woodrow [12] : outre quatre familles infinies (deux triviales, deux non-triviales), il y a un seul exemple sporadique, à savoir le graphe R !

Les graphes dirigés ultrahomogènes finis et infinis dénombrables ont été classés en 1982 et 1998.

Théorème (Georg Cantor [13] 1895). *L'ensemble ordonné* $(\mathbb{Q}, \leqslant)$ *est ultrahomogène.*

Démonstration. Si $x_1 < x_2 < \cdots < x_n$ et $y_1 < y_2 < \cdots < y_n$ sont des nombres rationnels, il y a une et une seule bijection de $\{x_1, \ldots, x_n\}$ sur $\{y_1, \ldots, y_n\}$ conservant la relation d'ordre, et on construit facilement un automorphisme α de $(\mathbb{Q}, \leqslant)$ qui étend cette bijection : il suffit de poser $\alpha(x_i) = y_i$ pour tout $i = 1, \ldots, n$ et de l'étendre par une fonction linéaire $x \mapsto ax + b$ sur chaque intervalle $[x_i, x_{i+1}]$. □

Notons que $(\mathbb{Q}, \leqslant)$ ne serait pas ultrahomogène si on autorisait, dans la définition de l'ultrahomogénéité, la prise en compte de sous-ensembles S_1 et S_2 infinis : en effet, si on prend par exemple $S_1 = \mathbb{Z}$ et

$$S_2 = \left\{ -1 + \frac{1}{2^k}, 1 - \frac{1}{2^k} \text{ t.q. } k \in \mathbb{N}_0 \right\}$$

il n'y a aucun automorphisme de $(\mathbb{Q}, \leqslant)$ appliquant S_1 sur S_2 puisque S_2 est borné et que S_1 ne l'est pas.

Voici un dernier exemple, plus classique : l'espace euclidien $\mathbb{R}^n$, vu comme espace métrique avec comme automorphismes les isométries, est ultrahomogène (exercice).

On trouvera d'autres exemples dans la thèse de doctorat d'Alice Devillers [14].

7 Bibliographie

[1] J.-P. Serre, *Cours d'arithmétique*, vol. 2 *in Collection SUP: "Le Mathématicien"*. Paris: Presses Universitaires de France, 1970.

[2] W. Sierpiński, « Sur les nombres premiers ayant des chiffres initiaux et finals donnés », *Acta Arith.*, vol. 5, p. 265–266, 1959.

[3] B. Green et T. Tao, « The primes contain arbitrarily long arithmetic progressions », *Ann. of Math. (2)*, vol. 167, no. 2, p. 481–547, 2008.

[4] M. Gerstenhaber, « The 152nd proof of the law of quadratic reciprocity », *Amer. Math. Monthly*, vol. 70, p. 397–398, 1963.

[5] P. Erdős et A. Rényi, « Asymmetric graphs », *Acta Math. Acad. Sci. Hungar*, vol. 14, p. 295–315, 1963.

[6] R. Rado, « Universal graphs and universal functions », *Acta Arith.*, vol. 9, p. 331–340, 1964.

[7] P. J. Cameron, *Permutation groups*, vol. 45 *in London Mathematical Society Student Texts*. Cambridge: Cambridge University Press, 1999.

[8] J. Sheehan, « Smoothly embeddable subgraphs », *J. London Math. Soc. (2)*, vol. 9, p. 212–218, 1974.

[9] A. Gardiner, « Homogeneous graphs », *J. Combinatorial Theory Ser. B*, vol. 20, no. 1, p. 94–102, 1976.

[10] J. J. Gol'fand et M. H. Klin, « On k-homogeneous graphs », *in Algorithmic studies in combinatorics (Russian)*, p. 76–85, 186 (errata insert), Moscow: "Nauka", 1978.

[11] C. Ronse, « On homogeneous graphs », *J. London Math. Soc. (2)*, vol. 17, no. 3, p. 375–379, 1978.

[12] A. H. Lachlan et R. E. Woodrow, « Countable ultrahomogeneous undirected graphs », *Trans. Amer. Math. Soc.*, vol. 262, no. 1, p. 51–94, 1980.

[13] G. Cantor, « Beiträge zur Begründung der transfiniten Mengenlehre », *Mathematische Annalen*, vol. 46, p. 481–512, 1895.

[14] A. Devillers, *Classification of some homogeneous and ultrahomogeneous structures*. Thèse de doctorat, ULB, 2002.