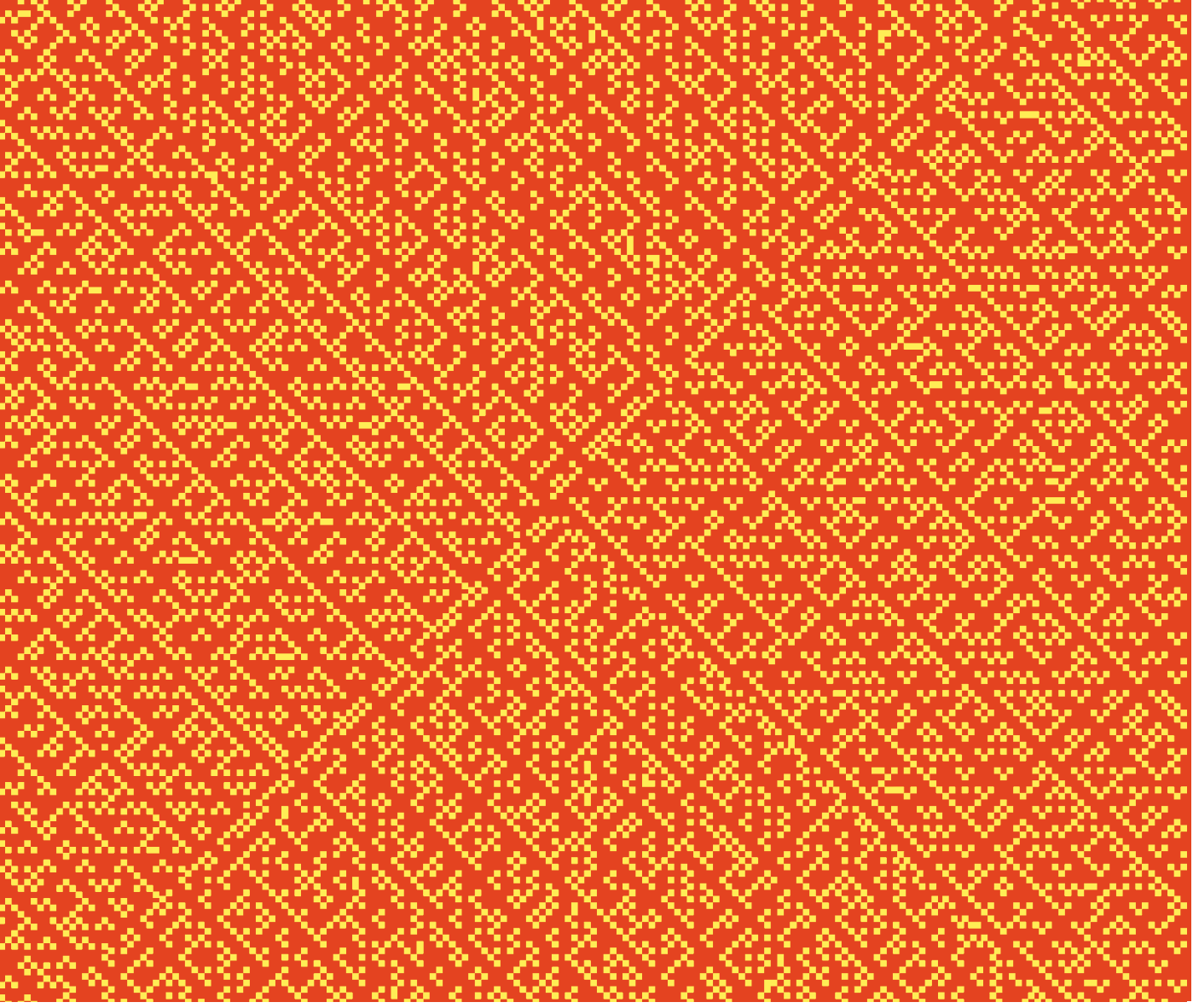


Formes mathématiques

La ronde des nombres premiers

Les nombres premiers, atomes de l'arithmétique, ont une répartition mystérieuse parmi les nombres entiers si on les écrit en ligne. Mais les représenter en utilisant une dimension de plus révèle (un peu) leur organisation : si on les dispose en spirale sur un quadrillage plan ou en hélice sur un cylindre, des alignements de nombres premiers apparaissent.

PAR **ROMAIN ATTAL** ET **GUILLAUME REUILLER**, MÉDIATEURS AU DÉPARTEMENT DE MATHÉMATIQUES DU PALAIS DE LA DÉCOUVERTE

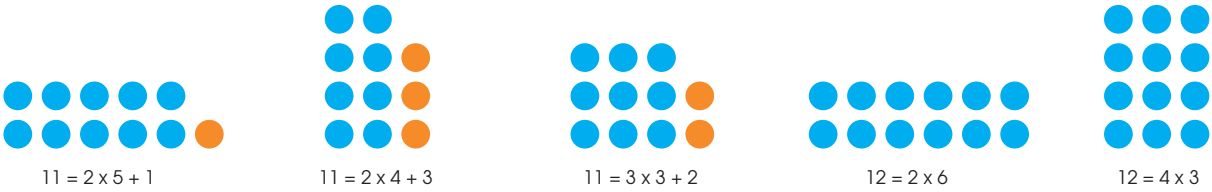


Figure 1. 11 est un nombre premier, contrairement à 12.

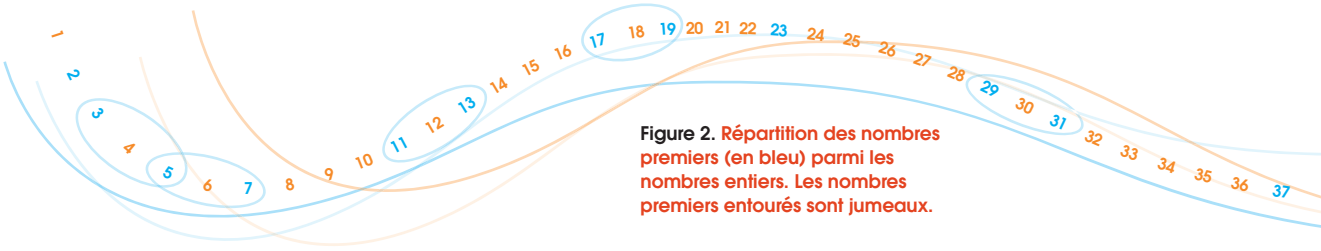


Figure 2. Répartition des nombres premiers (en bleu) parmi les nombres entiers. Les nombres premiers entourés sont jumeaux.

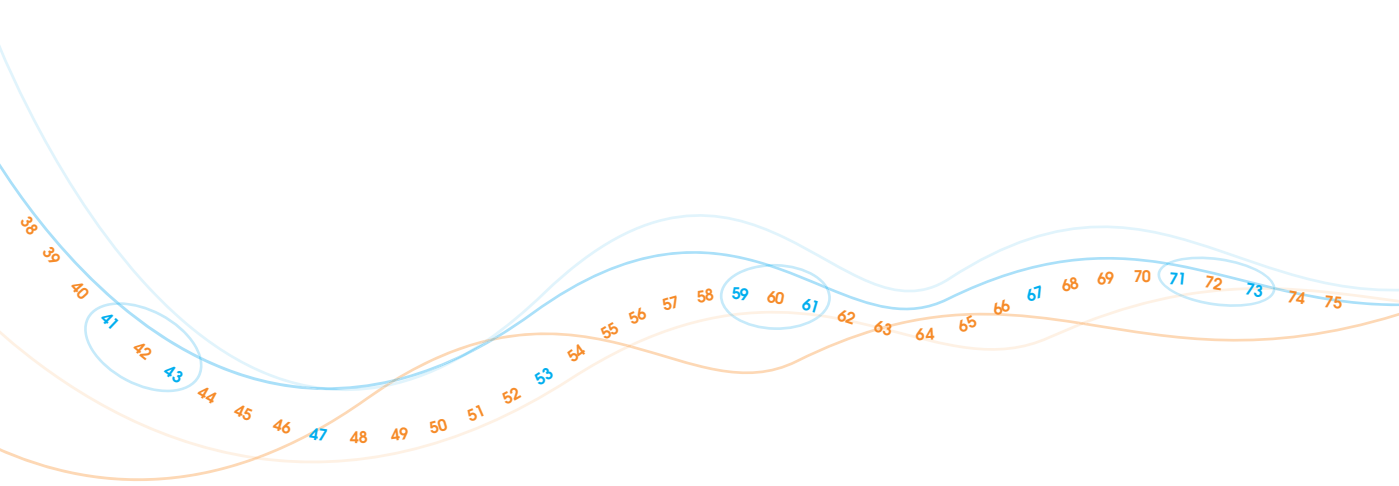
Lorsqu'un nombre entier *N* admet des diviseurs autres que 1 et lui-même, on dit qu'il est composé. Par exemple $6 = 2 \times 3$ est un nombre composé, divisible par 2 et par 3. Si, au contraire, on ne peut pas décomposer *N* comme un produit de nombres entiers différents de 1 et *N*, on dit que *N* est un nombre premier. En fait les nombres premiers sont ceux qui ont exactement deux diviseurs distincts (il serait gênant de ranger 1 parmi les nombres premiers). Voici une manière de représenter géométriquement les nombres premiers. En disposant *N* billes en un rectangle de côtés *a* et *b* (fig. 1), on décompose *N* en produit de *a* par *b*. Si *N* est premier, le seul rectangle possible est une ligne de longueur *N*.

EN NOMBRE INFINI, MAIS DE PLUS EN PLUS RARES

Depuis l'Antiquité grecque, nous savons qu'il existe une infinité de nombres premiers (encadré *Le théorème d'Euclide*). Cependant, ces derniers sont de plus en plus rares parmi les nombres entiers (fig. 2). Si *N* est un très grand nombre, le théorème de raréfaction des nombres premiers (conjecturé par Carl-Friedrich Gauss (1777-1855) et Adrien-Marie Legendre (1752-1833) à la fin du XVIII^{e} siècle, mais démontré indépendamment par Jacques Hadamard (1865-1963) et Charles de la Vallée-Poussin (1866-1962) en 1896) nous donne une estimation de la proportion de nombres premiers parmi les entiers plus petits que *N*. Notons *P(N)* le nombre d'entiers premiers inférieurs à *N*. Quand *N* augmente, le rapport *N/P(N)* devient de plus en plus grand et est approximativement proportionnel au nombre de chiffres de *N* (écrit, par exemple, dans le système décimal usuel). L'un des problèmes actuels les plus ardus de l'arithmétique est de comprendre plus précisément la répartition des nombres premiers. Certains problèmes ouverts semblent cependant plus accessibles. Par exemple, même si les nombres premiers sont, en moyenne, de plus en plus rares, ils peuvent parfois être très proches tout en étant « très grands », comme *2 760 889 966 649* et *2 760 889 966 651*. Deux tels nombres premiers, qui ne diffèrent que de 2, sont dits jumeaux. En utilisant le théorème de raréfaction des nombres premiers, on peut conjecturer qu'il existe une infinité de paires de nombres premiers jumeaux mais on n'en a pas encore de preuve rigoureuse.

LA SPIRALE DE KLAUBER-ULAM...

La répartition des nombres premiers, apparemment désordonnée, ne suit-elle pas pour autant des règles plus précises ? En particulier, peut-on trouver des formules simples qui nous fournissent des nombres premiers aussi grands que l'on veut ? Une piste suivie pour explorer ce mystère a été découverte en 1932 par Laurence Klauber (1883-1968), naturaliste américain, spécialiste des serpents à sonnette, puis redécouverte fortuitement en 1963 par le mathématicien



a)

65	64	63	62	61	60	59	58	57
66	37	36	35	34	33	32	31	56
67	38	17	16	15	14	13	30	55
68	39	18	5	4	3	12	29	54
69	40	19	6	1	2	11	28	53
70	41	20	7	8	9	10	27	52
71	42	21	22	23	24	25	26	51
72	43	44	45	46	47	48	49	50
73	74	75	76	77	78	79	80	81

b)

65	64	63	62	61	60	59	58	57
66	37	36	35	34	33	32	31	56
67	38	17	16	15	14	13	30	55
68	39	18	5	4	3	12	29	54
69	40	19	6	1	2	11	28	53
70	41	20	7	8	9	10	27	52
71	42	21	22	23	24	25	26	51
72	43	44	45	46	47	48	49	50
73	74	75	76	77	78	79	80	81

c)

65	64	63	62	61	60	59	58	57
66	37	36	35	34	33	32	31	56
67	38	17	16	15	14	13	30	55
68	39	18	5	4	3	12	29	54
69	40	19	6	1	2	11	28	53
70	41	20	7	8	9	10	27	52
71	42	21	22	23	24	25	26	51
72	43	44	45	46	47	48	49	50
73	74	75	76	77	78	79	80	81

Figure 3. Construction d'une spirale de 81 cases.

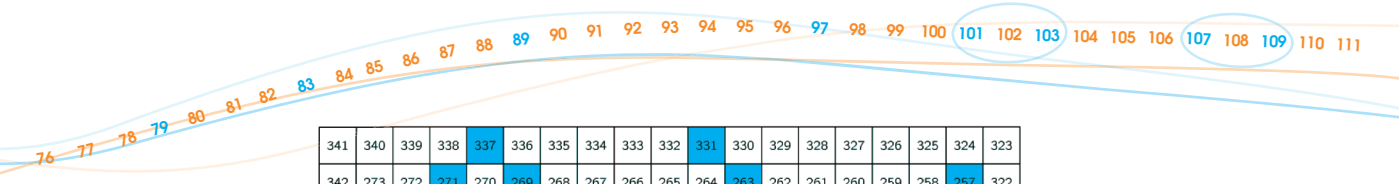
américain Stanislaw Ulam (1909-1984). Sur du papier quadrillé, numérotons les cases en spirale avec 1 au centre (fig. 3a) et marquons celles qui portent un nombre premier (fig. 3b). Si la spirale est assez longue, on peut alors voir apparaître de jolis alignements de nombres premiers, horizontaux, verticaux ou obliques (figure d'entrée). Il y a aussi des lignes totalement dépourvues de nombres premiers. Y a-t-il une loi mathématique qui explique ces alignements ?

... ET LES POLYNÔMES D'EULER

Remarquons d'abord (fig. 3c) que tous les carrés des nombres pairs (4, 16, 36, 64, ...) sont alignés en diagonale. De même pour les carrés des nombres impairs

Le théorème d'Euclide

La démonstration d'Euclide, du fait qu'il existe une infinité de nombres premiers, repose sur le théorème fondamental de l'arithmétique, selon lequel tout nombre entier se décompose de manière unique en un produit de nombres premiers (l'ordre des facteurs ne compte pas). Par exemple, $370 = 2 \times 5 \times 37$ ou $142\,857 = 3^3 \times 11 \times 13 \times 37$, où 2, 3, 5, 11, 13 et 37 sont premiers. Si p désigne un nombre premier quelconque, le nombre entier $q = 1 + (2 \times 3 \times 5 \times 7 \times \ldots \times p)$, successeur du produit de tous les nombres premiers inférieurs ou égaux à p, n'est divisible par aucun de ceux-là, puisque la division donne toujours 1 comme reste.
Les diviseurs premiers de q sont donc supérieurs à p. Pour tout nombre premier p, il existe donc des nombres premiers plus grands que p : l'ensemble des nombres premiers est bien infini.



341	340	339	338	337	336	335	334	333	332	331	330	329	328	327	326	325	324	323
342	273	272	271	270	269	268	267	266	265	264	263	262	261	260	259	258	257	322
343	274	213	212	211	210	209	208	207	206	205	204	203	202	201	200	199	256	321
344	275	214	161	160	159	158	157	156	155	154	153	152	151	150	149	198	255	320
345	276	215	162	117	116	115	114	113	112	111	110	109	108	107	148	197	254	319
346	277	216	163	118	81	80	79	78	77	76	75	74	73	106	147	196	253	318
347	278	217	164	119	82	53	52	51	50	49	48	47	72	105	146	195	252	317
348	279	218	165	120	83	54	33	32	31	30	29	46	71	104	145	194	251	316
349	280	219	166	121	84	55	34	21	20	19	28	45	70	103	144	193	250	315
350	281	220	167	122	85	56	35	22	17	18	27	44	69	102	143	192	249	314
351	282	221	168	123	86	57	36	23	24	25	26	43	68	101	142	191	248	313
352	283	222	169	124	87	58	37	38	39	40	41	42	67	100	141	190	247	312
353	284	223	170	125	88	59	60	61	62	63	64	65	66	99	140	189	246	311
354	285	224	171	126	89	90	91	92	93	94	95	96	97	98	139	188	245	310
355	286	225	172	127	128	129	130	131	132	133	134	135	136	137	138	187	244	309
356	287	226	173	174	175	176	177	178	179	180	181	182	183	184	185	186	243	308
357	288	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	307
358	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306
359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377

Figure 4. Une spirale centrée sur 17.

(1, 9, 25, 49, ...). La ligne horizontale qui commence par 1, 6, 19, 40, 69, ... contient, quant à elle, les nombres de la forme $4n^2 + n + 1$ pour $n = 0, 1, 2, 3, 4, \ldots$ Plus généralement, à chaque alignement de cases issu du centre de la spirale correspond un polynôme $f(n) = an^2 + bn + c$, tel que la énième case contienne le nombre $f(n)$.

En 1752, Christian Goldbach (1690-1764) a démontré qu'il n'existait aucun polynôme $g(n)$ qui ne donne que des nombres premiers lorsque n parcourt l'ensemble des nombres entiers. Par conséquent, dans notre spirale, aucune ligne, colonne ou diagonale ne peut contenir que des nombres premiers : il y a forcément des interruptions dans ces alignements. Néanmoins, il existe des polynômes qui nous donnent successivement beaucoup de nombres premiers. Par exemple, Leonhard Euler (1707-1783) a découvert que le polynôme $f_{41}(n) = n^2 + n + 41$ donnait 40 nombres premiers lorsque n variait de 0 à 39.

Plaçons maintenant 17 au centre de la spirale (fig. 4). Cela permet d'aligner des nombres premiers qui ne l'étaient pas quand 1 était au centre, comme 17, 19, 23, 29 et 47, qui sont les valeurs de $f_{17}(n) = n^2 + n + 17$ en $n = 0, 1, 2, 3$ et 4. Cette séquence de nombres premiers est rompue par 289 et 323, mais de nouveaux nombres premiers, comme 359, apparaissent ensuite. Plus généralement, si $p = 2, 3, 5, 11, 17, 41$, le polynôme $f_p(n) = n^2 + n + p$ (appelé polynôme d'Euler) donne $p - 1$ nombres premiers consécutifs lorsque n varie de 0 à $p - 2$. Puisque $f_p(p - 1) = (p - 1)^2 + (p - 1) + p = p^2$ n'est pas premier, l'alignement correspondant s'interrompt en $n = p - 1$. Ensuite, de nouveaux nombres premiers apparaissent sporadiquement.

QUELQUES QUESTIONS EN SUSPENS

Stanislaw Ulam et ses collaborateurs ont constaté que 47,5 % des nombres de la forme $n^2 + n + 41$ inférieurs à dix millions étaient des nombres premiers. En se limitant aux valeurs de n inférieures à quelques milliers, on trouve que certains polynômes de degré 2 sont généreux en nombres premiers ($4n^2 + 4n + 59$ en donne 43,7 %), tandis que d'autres sont plutôt pingres en la matière ($2n^2 + 4n + 117$ n'en donne que 5 %). Mais y a-t-

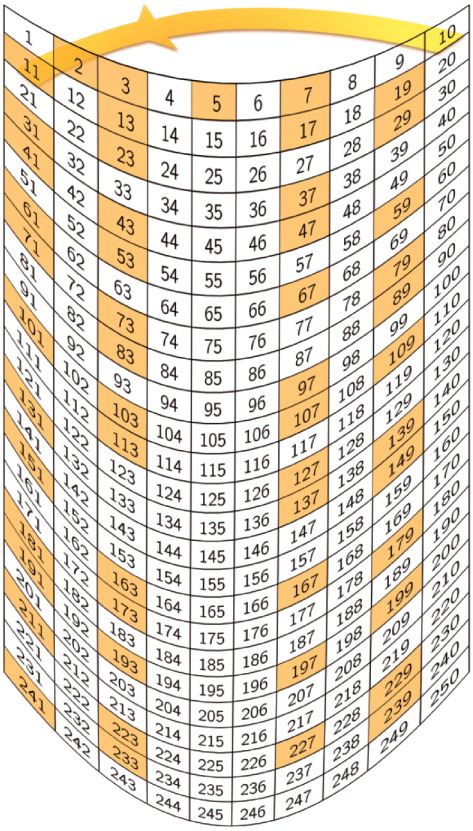


Figure 5. En identifiant les côtés verticaux de ce rectangle, on obtient un cylindre de périmètre 10. Les nombres premiers sont en orange.

il pour autant une infinité de nombres premiers dans chaque ligne du quadrillage ? Quelle est alors la proportion maximale de nombres premiers dans ces lignes ? Ces questions n'ont pas encore de réponse... On connaît aussi des polynômes de degré supérieur qui donnent des suites plus ou moins longues de nombres premiers, mais on ne dispose pas aujourd'hui d'explication générale de ce phénomène. Le dernier record en date vient d'être établi (en septembre 2010) par deux mathématiciens français, Bernard Landreau et François Dress. Leur polynôme $P(n) = (1/72)n^6 - (5/24)n^5 - (1\,493/72)n^4 + (1\,027/8)n^3 + (100\,471/18)n^2 - (11\,971/6)n - 57\,347$ fournit 58 nombres premiers lorsque l'entier n varie de –42 à +15.

SUR UN CYLINDRE

En disposant les nombres entiers en hélice autour d'un cylindre de périmètre a, les nombres alignés suivant l'axe du cylindre diffèrent d'un multiple de a (la figure 5 illustre le cas où $a = 10$). On dit qu'ils forment une suite arithmétique de raison a. Un théorème (1837) de Gustav Dirichlet (1805-1859) nous dit que si a et b sont deux entiers qui n'ont que 1 comme diviseur commun, alors la suite $(b, a + b, 2a + b, 3a + b, ...)$ contient une infinité de nombres premiers. Ainsi, quel que soit l'entier a, périmètre du cylindre, et pour tout nombre b qui n'a que 1 comme diviseur commun avec a, la ligne issue de b contient une infinité de nombres premiers. Ces derniers peuvent être très espacés et très éloignés les uns des autres : lorsqu'ils arrivent dans cette suite, c'est la surprise ! Sur la figure 5, le cylindre a pour périmètre $10 = 2 \times 5$, donc si b est un entier qui n'est divisible ni par 2 ni par 5, il existe une infinité de nombres premiers dans la suite arithmétique $(b, b + 10, b + 20, b + 30, ...)$. C'est le cas pour $b = 1, 3, 7$ et 9. On trouve donc facilement des suites arithmétiques contenant une infinité de nombres premiers. Mais s'il existait une suite arithmétique infinie constituée uniquement de nombres premiers, ces derniers apparaîtraient régulièrement parmi les nombres entiers, ce qui contredirait le théorème de raréfaction.

LE THÉORÈME DE GREEN-TAO

Voici une autre question, proche de la précédente : peut-on trouver des suites de nombres premiers espacés régulièrement (comme 109, 219, 329, 439, 549, 659 et 769) et de n'importe quelle longueur ? La réponse, positive, a été donnée en 2004 par Ben Green (1977-) et Terence Tao (1975-) : il existe bien des suites arithmétiques de nombres premiers de toutes longueurs. La preuve du théorème de Green-Tao, qui utilise essentiellement la théorie des probabilités, ne donne malheureusement pas de méthode pour construire ces suites. En particulier, rien n'est dit sur la différence entre deux termes successifs ni sur le premier terme, en fonction de la longueur de la suite. **R. A. ET G. R.**

Pour en savoir plus

Hardy G. H., Wright E. M., *Introduction à la théorie des nombres*, Paris, Éditions Vuibert/Springer, 2006.

Pour aller plus loin

Les nombres de Heegner*

Le théorème fondamental de l'arithmétique nous dit que tout nombre entier se décompose de manière unique en produit de facteurs premiers. Plus généralement, un ensemble *F*, muni d'une multiplication, dans lequel tout élément se décompose de manière unique en un produit de facteurs indécomposables dans *F* est dit factoriel. L'ensemble des entiers est donc factoriel. Voici un exemple simple d'ensemble non factoriel dû à David Hilbert (1862-1943). L'ensemble $H = \{1, 5, 9, 13, 17, 21, 25, 29, ...\}$ des entiers de la forme $4n + 1$ est stable par multiplication : le produit de deux éléments de *H* est encore un élément de *H* puisque $(4m + 1)(4n + 1) = 4(4mn + m + n) + 1$. Mais *H* n'est pas factoriel ! En effet, tandis que *25* se décompose uniquement en 5×5, *441* ne se décompose pas de façon unique dans *H* car $441 = 21 \times 21 = 9 \times 49$ (on vérifie aisément que *5, 9, 21* et *49* sont bien des éléments indécomposables dans *H*). Voici un autre exemple de (non-)factorialité. Notons $Z[i\sqrt{d}]$ l'ensemble des nombres complexes de la forme $a + ib\sqrt{d}$, avec *a*, *b* et *d* entiers, *d* n'ayant pas de diviseur carré et *i* vérifiant $i^2 = -1$. Ces nombres forment un réseau rectangulaire dans le plan complexe (fig. I). Pour la plupart des valeurs de *d*, la décomposition en produit de facteurs indécomposables n'est pas unique dans $Z[i\sqrt{d}]$. Par exemple, pour $d = 5$, on a $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ avec 3, $2 + i\sqrt{5}$, et $2 - i\sqrt{5}$ indécomposables dans $Z[i\sqrt{5}]$. Les seules valeurs de *d* pour lesquelles $Z[i\sqrt{d}]$ est factoriel sont appelées les nombres de Heegner : $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$. Nous avons vu que pour $p = 2, 3, 5, 11, 17, 41$, le polynôme $f_p(n) = n^2 + n + p$ donnait $p - 1$ nombres premiers consécutifs lorsque *n* varie de *0* à $p - 2$. Ces valeurs de *p* sont reliées aux nombres de Heegner de la manière suivante. Le discriminant du polynôme $f_p(n) = n^2 + n + p$ est $D = 1 - 4p$. Si $p = 2, 3, 5, 11, 17, 41$, alors $4p - 1 = 7, 11, 19, 43, 67, 163$: ce sont les six derniers nombres de Heegner, les seuls de la forme $4p - 1$. Les nombres de Heegner ont encore bien d'autres propriétés remarquables que l'on découvrira en lisant un bon manuel de théorie des nombres.

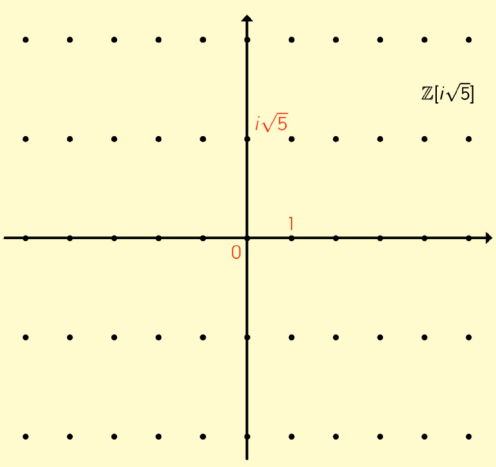


Figure I. Le réseau rectangulaire $Z[i\sqrt{5}]$.

* Kurt Heegner (1893-1963) est connu pour ses travaux en théorie algébrique des nombres, en particulier pour la résolution du « problème du nombre de classe 1» formulé par Gauss.