Une petite[1] histoire des nombres premiers

Vieux problèmes et percées récentes

Jean-Robert Belliard

IREM Franche-Comté

[1] Merci à Nicolas Jacon

I. VIEUX PROBLÈMES

Qu'est ce qu'un nombre premier ?

Qu'est ce qu'un nombre premier ?

C'est un entier naturel strictement supérieur à 1, n'admettant que deux entiers naturels diviseurs distincts: 1 et lui-même.

Qu'est ce qu'un nombre premier ?

C'est un entier naturel strictement supérieur à 1, n'admettant que deux entiers naturels diviseurs distincts: 1 et lui-même.

Par exemple $6 = 2 \times 3$. On dit que 2 divise 6, que 3 divise aussi 6.

Qu'est ce qu'un nombre premier ?

C'est un entier naturel strictement supérieur à 1, n'admettant que deux entiers naturels diviseurs distincts: 1 et lui-même.

Par exemple $6 = 2 \times 3$. On dit que 2 divise 6, que 3 divise aussi 6.

6 n'est pas premier.

Qu'est ce qu'un nombre premier ?

C'est un entier naturel strictement supérieur à 1, n'admettant que deux entiers naturels diviseurs distincts: 1 et lui-même.
Par exemple $6 = 2 \times 3$. On dit que 2 divise 6, que 3 divise aussi 6.

6 n'est pas premier.

On peut toujours écrire $2 = 1 \times 2$ et $3 = 1 \times 3$ mais ce sont les seules divisions possibles.

Qu'est ce qu'un nombre premier ?

C'est un entier naturel strictement supérieur à 1, n'admettant que deux entiers naturels diviseurs distincts: 1 et lui-même.
Par exemple $6 = 2 \times 3$. On dit que 2 divise 6, que 3 divise aussi 6.

6 n'est pas premier.

On peut toujours écrire $2 = 1 \times 2$ et $3 = 1 \times 3$ mais ce sont les seules divisions possibles.

2 et 3 sont premiers.

Qu'est ce qu'un nombre premier ?

C'est un entier naturel strictement supérieur à 1, n'admettant que deux entiers naturels diviseurs distincts: 1 et lui-même.
Par exemple $6 = 2 \times 3$. On dit que 2 divise 6, que 3 divise aussi 6.

6 n'est pas premier.

On peut toujours écrire $2 = 1 \times 2$ et $3 = 1 \times 3$ mais ce sont les seules divisions possibles.

2 et 3 sont premiers.

Ces nombres ont une importance centrale en mathématiques : on peut montrer que tout entier naturel peut se décomposer en produit d'un ou de plusieurs facteurs premiers.

Par exemple, $42 = 2 \times 3 \times 7$ ou $180 = 2 \times 2 \times 3 \times 3 \times 5$.

Par exemple, $42 = 2 \times 3 \times 7$ ou $180 = 2 \times 2 \times 3 \times 3 \times 5$.

Les nombres premiers peuvent donc être vu comme les composantes de base des nombres entiers.

La simplicité de cette définition ainsi que l'apparente importance de ce concept ont amené les mathématiciens à s'y intéresser dès l'antiquité.

Par exemple, $42 = 2 \times 3 \times 7$ ou $180 = 2 \times 2 \times 3 \times 3 \times 5$.
Les nombres premiers peuvent donc être vu comme les composantes de base des nombres entiers.
La simplicité de cette définition ainsi que l'apparente importance de ce concept ont amené les mathématiciens à s'y intéresser dès l'antiquité.
C'est aussi une des occurences les plus anciennes d'une démarches générale en maths et en sciences exactes : Pour comprendre un objet compliqué (ici un nombre) on le décompose en "particules élémentaires" (ici des nombres premiers). Puis on classifie ces particules élémentaires ...

Par exemple, $42 = 2 \times 3 \times 7$ ou $180 = 2 \times 2 \times 3 \times 3 \times 5$.
Les nombres premiers peuvent donc être vu comme les composantes de base des nombres entiers.
La simplicité de cette définition ainsi que l'apparente importance de ce concept ont amené les mathématiciens à s'y intéresser dès l'antiquité.
C'est aussi une des occurences les plus anciennes d'une démarches générale en maths et en sciences exactes : Pour comprendre un objet compliqué (ici un nombre) on le décompose en "particules élémentaires" (ici des nombres premiers). Puis on classifie ces particules élémentaires ...
La plupart des grands noms des mathématiques se sont penchés sur des questions liées aux nombres premiers: Euclide, Fermat, Pascal, Euler, Gauss, Legendre, Riemann, Hilbert, ... Turing.

Voici la liste des nombres premiers inférieur à 100 :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71,$$

$$73, 79, 83, 89, 97$$

Problème naturel :

Voici la liste des nombres premiers inférieur à 100 :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71,$$

$$73, 79, 83, 89, 97$$

Problème naturel : Combien y a t-il de nombres premiers ?

Voici la liste des nombres premiers inférieur à 100 :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71,$$

$$73, 79, 83, 89, 97$$

Problème naturel : Combien y a t-il de nombres premiers ?

Réponse : Une infinité ! (une démonstration due à Euclide)

Voici la liste des nombres premiers inférieur à 100 :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71,$$

$$73, 79, 83, 89, 97$$

Problème naturel : Combien y a t-il de nombres premiers ?

Réponse : Une infinité ! (une démonstration due à Euclide)

Un autre problème naturel:

Voici la liste des nombres premiers inférieur à 100 :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71,$$

$$73, 79, 83, 89, 97$$

Problème naturel : Combien y a t-il de nombres premiers ?
Réponse : Une infinité ! (une démonstration due à Euclide)

Un autre problème naturel: Y a t-il une règle gouvernant la succession des nombres premiers ?
Réponse: Cette question est reliée à l'Hypothèse de Riemann. Les plus grands mathématiciens se sont confrontés à cette conjecture depuis plus d'un siècle ...

Voici la liste des nombres premiers inférieur à 100 :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71,$$

$$73, 79, 83, 89, 97$$

Problème naturel : Combien y a t-il de nombres premiers ?
Réponse : Une infinité ! (une démonstration due à Euclide)

Un autre problème naturel: Y a t-il une règle gouvernant la succession des nombres premiers ?
Réponse: Cette question est reliée à l'Hypothèse de Riemann. Les plus grands mathématiciens se sont confrontés à cette conjecture depuis plus d'un siècle ... sans succès.

Une des raisons rendant ce concept aussi fascinant vient aussi du fait que beaucoup de problèmes à l'énoncé relativement simple se sont révélés tres ardues à résoudre. Les deux problèmes suivants, par exemple, restent également des problèmes ouverts :

Une des raisons rendant ce concept aussi fascinant vient aussi du fait que beaucoup de problèmes à l'énoncé relativement simple se sont révélés tres ardues à résoudre. Les deux problèmes suivants, par exemple, restent également des problèmes ouverts :

La conjecture de Goldbach : tout nombre pair supérieur ou égal à 6, peut-il s'écrire comme somme de deux nombres premiers ?

Une des raisons rendant ce concept aussi fascinant vient aussi du fait que beaucoup de problèmes à l'énoncé relativement simple se sont révélés tres ardues à résoudre. Les deux problèmes suivants, par exemple, restent également des problèmes ouverts :

La conjecture de Goldbach : tout nombre pair supérieur ou égal à 6, peut-il s'écrire comme somme de deux nombres premiers ?

La conjecture des nombres premiers jumeaux : un couple de nombres premiers jumeaux est une paire de nombres premiers dont la différence est égale à 2. Existe-t-il une infinité de jumeaux premiers ?

Une des raisons rendant ce concept aussi fascinant vient aussi du fait que beaucoup de problèmes à l'énoncé relativement simple se sont révélés tres ardues à résoudre. Les deux problèmes suivants, par exemple, restent également des problèmes ouverts :

La conjecture de Goldbach : tout nombre pair supérieur ou égal à 6, peut-il s'écrire comme somme de deux nombres premiers ?

La conjecture des nombres premiers jumeaux : un couple de nombres premiers jumeaux est une paire de nombres premiers dont la différence est égale à 2. Existe-t-il une infinité de jumeaux premiers ?

La difficulté des ces problèmes a fait dire à Paul Erdös "Dieu ne joue peut-être pas aux dés avec l'univers, mais il se passe quelque chose d'étrange avec les nombres premiers"

D'autre part, la recherche sur ces nombres premiers a toujours été très active dans l'histoire des mathématiques. L'étude de l'histoire des nombres premiers permet de percevoir comment la discipline a évolué aux cours des siècles.

D'autre part, la recherche sur ces nombres premiers a toujours été très active dans l'histoire des mathématiques. L'étude de l'histoire des nombres premiers permet de percevoir comment la discipline a évolué aux cours des siècles.

Enfin, il s'est avéré que cette branche des mathématiques avait de nombreux applications, dont certaines plutôt surprenantes comme en informatique ou en Physique quantique.

D'autre part, la recherche sur ces nombres premiers a toujours été très active dans l'histoire des mathématiques. L'étude de l'histoire des nombres premiers permet de percevoir comment la discipline a évolué aux cours des siècles.

Enfin, il s'est avéré que cette branche des mathématiques avait de nombreux applications, dont certaines plutôt surprenantes comme en informatique ou en Physique quantique.

Mais au fait comment obtenir la liste :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71,$$

$$73, 79, 83, 89, 97 \ ?$$

II. LE CRIBLE D'ÉRATOSTÈNE

En langage actuel, voici le fonctionnement de cet crible. On commence par écrire la liste de tous les nombres jusqu'à n.

En langage actuel, voici le fonctionnement de cet crible. On commence par écrire la liste de tous les nombres jusqu'à n.

- On élimine 1.

En langage actuel, voici le fonctionnement de cet crible. On commence par écrire la liste de tous les nombres jusqu'à n.

- On élimine 1.
- On souligne 2 et on élimine tous les multiples de 2.

En langage actuel, voici le fonctionnement de cet crible. On commence par écrire la liste de tous les nombres jusqu'à n.

- On élimine 1.
- On souligne 2 et on élimine tous les multiples de 2.
- 3 est le plus petit nombre non éliminé : on le souligne et on élimine tous les multiples de 3.

En langage actuel, voici le fonctionnement de cet crible. On commence par écrire la liste de tous les nombres jusqu'à n.

- On élimine 1.
- On souligne 2 et on élimine tous les multiples de 2.
- 3 est le plus petit nombre non éliminé : on le souligne et on élimine tous les multiples de 3.
- On choisit alors le plus petit nombre non souligné et non éliminé, c'est 5. On élimine tous ses multiples.

En langage actuel, voici le fonctionnement de cet crible. On commence par écrire la liste de tous les nombres jusqu'à n.

- On élimine 1.
- On souligne 2 et on élimine tous les multiples de 2.
- 3 est le plus petit nombre non éliminé : on le souligne et on élimine tous les multiples de 3.
- On choisit alors le plus petit nombre non souligné et non éliminé, c'est 5. On élimine tous ses multiples.
- On réitère le procédé jusqu'au nombre m tel que $(m+1) \times (m+1) > n$.

En langage actuel, voici le fonctionnement de cet crible. On commence par écrire la liste de tous les nombres jusqu'à n.

- On élimine 1.
- On souligne 2 et on élimine tous les multiples de 2.
- 3 est le plus petit nombre non éliminé : on le souligne et on élimine tous les multiples de 3.
- On choisit alors le plus petit nombre non souligné et non éliminé, c'est 5. On élimine tous ses multiples.
- On réitère le procédé jusqu'au nombre m tel que $(m+1) \times (m+1) > n$.

Les nombres non éliminés sont les nombres premiers jusqu'à n.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

	$\underline{2}$	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

	$\underline{2}$	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

	2	$\underline{3}$		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

	2	3		$\underline{5}$		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

	2	3		$\underline{5}$		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

	2	3		5		$\underline{7}$			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

	2	3		5		$\underline{7}$			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

“ Ceux qui ne se laissent mesurer d’aucune façon, échappant ainsi à la mesure, sont les nombres premiers et non composés, qui se trouvent ainsi séparés du reste comme par un crible”

Le problème de cette méthode est qu'elle demande une mémoire beaucoup trop importante pour avoir des tables de grands nombres premiers.

Le problème de cette méthode est qu'elle demande une mémoire beaucoup trop importante pour avoir des tables de grands nombres premiers. A l'heure actuelle, on dispose de méthodes plus efficaces pour tester la primalité d'un nombre

Le problème de cette méthode est qu'elle demande une mémoire beaucoup trop importante pour avoir des tables de grands nombres premiers. A l'heure actuelle, on dispose de méthodes plus efficaces pour tester la primalité d'un nombre . Par exemple, on sait tester si un nombre premier de 100 chiffres est premier alors qu'un ordinateur de la taille du système solaire ne parviendrait pas à stocker tous les nombres premiers inférieurs à un tel nombre !

III. DEUX PERCÉES RÉCENTES

La conjecture des nombres premiers jumeaux : un couple de nombres premiers jumeaux est une paire de nombres premiers p et q avec $q = p + 2$. Existe-t-il une infinité de jumeaux premiers ?

La conjecture des nombres premiers jumeaux : un couple de nombres premiers jumeaux est une paire de nombres premiers p et q avec $q = p + 2$. Existe-t-il une infinité de jumeaux premiers ?
Une autre formulation (les mathématiques sont l'art d'appeler différemment des choses identiques) :

La conjecture des nombres premiers jumeaux : un couple de nombres premiers jumeaux est une paire de nombres premiers p et q avec $q = p + 2$. Existe-t-il une infinité de jumeaux premiers ?
Une autre formulation (les mathématiques sont l'art d'appeler différemment des choses identiques) :
Existe-t'il une infinité de nombres premier p et q tels que

$$p < q < p + 3 \quad ?$$

La conjecture des nombres premiers jumeaux : un couple de nombres premiers jumeaux est une paire de nombres premiers p et q avec $q = p + 2$. Existe-t-il une infinité de jumeaux premiers ?
Une autre formulation (les mathématiques sont l'art d'appeler différemment des choses identiques) :
Existe-t'il une infinité de nombres premier p et q tels que

$$p < q < p + 3 \quad ?$$

Une avancée spectaculaire en mai 2013 :

Théorème (Zhang)

Il existe une infinité de nombres premiers p et q tels que

$$p < q < p + 70\ 000\ 000\ .$$

Voici un extrait d'un article (disponible en ligne) du Journal de la Science :

Voici un extrait d'un article (disponible en ligne) du Journal de la Science :

Un mathématicien chinois a effectué un grand pas vers la démonstration d'un célèbre problème mathématique : la conjecture des nombres premiers jumeaux.

Ce qui est peut-être l'un des plus vieux problème mathématique pourrait bientôt être résolu grâce aux travaux d'un mathématicien chinois. En effet, Yitang Zhang (Université du New Hampshire, Etats-Unis) a réalisé une démonstration mathématique qui constitue un grand pas vers la validitation de la célèbre conjecture des nombres premiers jumeaux. Conjecture qui, selon plusieurs historiens des sciences, aurait été formulée par le célèbre mathématicien grec Euclide lui-même, quelques 3 siècles avant notre ère...

Conjecture de Goldbach : tout nombre pair supérieur ou égal à 6, peut-il s'écrire comme somme de deux nombres premiers ?

Conjecture de Goldbach : tout nombre pair supérieur ou égal à 6, peut-il s'écrire comme somme de deux nombres premiers ?

Quand on ne reformule pas on peut aussi affablir.

Conjecture de Goldbach : tout nombre pair supérieur ou égal à 6, peut-il s'écrire comme somme de deux nombres premiers ?

Quand on ne reformule pas on peut aussi affablir.

Conjecture de Goldbach faible: tout nombre impair supérieur ou égal à 9, peut-il s'écrire comme somme de trois nombres premiers ?

Conjecture de Goldbach : tout nombre pair supérieur ou égal à 6, peut-il s'écrire comme somme de deux nombres premiers ?

Quand on ne reformule pas on peut aussi affablir.

Conjecture de Goldbach faible: tout nombre impair supérieur ou égal à 9, peut-il s'écrire comme somme de trois nombres premiers ?

Théorème (HELFGOTT)

La Conjecture de Goldbach faible est vraie.

The proof given here works for all $n \geqslant C = 10^{29}$ ...
On complète avec des calculs sous ordinateurs !

Merci pour votre attention !