Histoire des nombres premiers

$1^{\text{ère}}$ partie : Les nombres premiers de l'antiquité à Riemann

N. Jacon

Université de Franche-Comté

I. INTRODUCTION

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. 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.

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. 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 est égale à $3 \times 7 \times 2$ ou $180 = 3^2 \times 2^2 \times 5$.

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. 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 est égale à $3 \times 7 \times 2$ ou $180 = 3^2 \times 2^2 \times 5$.

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.

La plupart des grands noms des mathématiques se sont penchés sur des questions liées à ces nombres : Euclide, Fermat, Pascal, Euler, Gauss, Legendre, Riemann, Hilbert, ... Turing.

La plupart des grands noms des mathématiques se sont penchés sur des questions liées à ces nombres : 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 :

La plupart des grands noms des mathématiques se sont penchés sur des questions liées à ces nombres : 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 : Combien y a t-il de nombres premiers ?

La plupart des grands noms des mathématiques se sont penchés sur des questions liées à ces nombres : 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 : Combien y a t-il de nombres premiers ?
Réponse : Une infinité ! (Euclide, cf la démonstration plus tard)

La plupart des grands noms des mathématiques se sont penchés sur des questions liées à ces nombres : 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 : Combien y a t-il de nombres premiers ?
Réponse : Une infinité ! (Euclide, cf la démonstration plus tard)

Un autre problème naturel:

La plupart des grands noms des mathématiques se sont penchés sur des questions liées à ces nombres : 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 : Combien y a t-il de nombres premiers ?
Réponse : Une infinité ! (Euclide, cf la démonstration plus tard)

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 ...

La plupart des grands noms des mathématiques se sont penchés sur des questions liées à ces nombres : 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 : Combien y a t-il de nombres premiers ?
Réponse : Une infinité ! (Euclide, cf la démonstration plus tard)

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 strictement supérieur à 2, 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 strictement supérieur à 2, 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 strictement supérieur à 2, 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.

II. LES NOMBRES PREMIERS, BASE DE L'ARITHMETIQUE

Les plus anciennes traces des nombres premiers ont été trouvées près du lac Edouard au Zaïre sur un os de plus de 20.000 ans, appelé l'os d'Ishango et recouvert d'entailles marquant les nombres 11, 13, 17 et 19. Ces nombres sont premiers : Est-ce un hasard ou l'ébauche d'une table de nombres premiers ?

Les plus anciennes traces des nombres premiers ont été trouvées près du lac Edouard au Zaïre sur un os de plus de 20.000 ans, appelé l'os d'Ishango et recouvert d'entailles marquant les nombres 11, 13, 17 et 19. Ces nombres sont premiers : Est-ce un hasard ou l'ébauche d'une table de nombres premiers ?

Plus tard, les grecs de l'Ecole Pythagoricienne, passionnés par l'Arithmétique, étudieront la notion de diviseur et les nombres parfaits (nombre égal à la somme de ses diviseurs propres).

Les plus anciennes traces des nombres premiers ont été trouvées près du lac Edouard au Zaïre sur un os de plus de 20.000 ans, appelé l'os d'Ishango et recouvert d'entailles marquant les nombres 11, 13, 17 et 19. Ces nombres sont premiers : Est-ce un hasard ou l'ébauche d'une table de nombres premiers ?

Plus tard, les grecs de l'Ecole Pythagoricienne, passionnés par l'Arithmétique, étudieront la notion de diviseur et les nombres parfaits (nombre égal à la somme de ses diviseurs propres).

Par exemple, 6 est un nombre parfait, car $6 = 1 + 2 + 3$, 1, 2 et 3 étant les diviseurs de 6. La notion de nombre premiers, voisine de celle-ci devait donc déjà être connue par Pythagore et ses adeptes.

La première allusion concrète aux nombres premiers est faite par Aristote dans un passage de ses *Seconds analytiques*:

La première allusion concrète aux nombres premiers est faite par Aristote dans un passage de ses *Seconds analytiques*:

"Sont par soi, en premier lieu les attributs qui appartiennent à l'essence du sujet : c'est ainsi qu'au triangle appartient la ligne et à la ligne le point (car la substance du triangle et de la ligne est composé de ces éléments, lesquels entrent dans la définition exprimant l'essence des choses)

La première allusion concrète aux nombres premiers est faite par Aristote dans un passage de ses *Seconds analytiques*:

"Sont par soi, en premier lieu les attributs qui appartiennent à l'essence du sujet : c'est ainsi qu'au triangle appartient la ligne et à la ligne le point (car la substance du triangle et de la ligne est composé de ces éléments, lesquels entrent dans la définition exprimant l'essence des choses). En second lieu, ce sont les attributs contenus dans les sujets qui sont eux-même compris dans la définition exprimant la nature de ces attributs : c'est ainsi que le rectiligne et le rond appartiennent à la ligne, le pair et l'impair, le premier et le composé, le carré [...] au nombre; et, pour tous ces attributs, la définition qui exprime leur nature contient le sujet, à savoir tantôt la ligne, tantôt le nombre."

En termes simple, Aristote associe à un objet deux types d'attributs :

- ces constituants (la ligne est composée de points) qui sont nécessaire à son existence.

En termes simple, Aristote associe à un objet deux types d'attributs :

- ces constituants (la ligne est composée de points) qui sont nécessaire à son existence.
- ces "propriétés caractéristiques" : la ligne peut être un rond ou être rectiligne, la parité ou l'imparité appartient au nombre, de même que la primalité ou la non-primalité appartient à celui-ci.

En termes simple, Aristote associe à un objet deux types d'attributs :

- ces constituants (la ligne est composée de points) qui sont nécessaire à son existence.
- ces "propriétés caractéristiques" : la ligne peut être un rond ou être rectiligne, la parité ou l'imparité appartient au nombre, de même que la primalité ou la non-primalité appartient à celui-ci.

Mais c'est véritablement avec Euclide que les bases de l'Arithmétique (et même des mathématiques !) vont être posées avec ses *"Eléments"*. C'est dans ce livre où l'on trouve la première notion de définitions, de démonstrations où la rigueur logique est de mise.

Voici un extrait du livre Septième :

Voici un extrait du livre Septième :

- “L’unité est ce selon quoi chacune des choses existentes est dite une

Voici un extrait du livre Septième :

- “L’unité est ce selon quoi chacune des choses existentes est dite une
- Un nombre est un assemblage composé d’unité,

Voici un extrait du livre Septième :

- “L’unité est ce selon quoi chacune des choses existentes est dite une
- Un nombre est un assemblage composé d’unité,
- Un nombre est une partie d’un nombre, le plus petit du plus grand, lorsque le plus petit mesure le plus grand,

Voici un extrait du livre Septième :

- “L’unité est ce selon quoi chacune des choses existentes est dite une
- Un nombre est un assemblage composé d’unité,
- Un nombre est une partie d’un nombre, le plus petit du plus grand, lorsque le plus petit mesure le plus grand,
- Le nombre premier est celui qui est mesuré par l’unité seul,

Voici un extrait du livre Septième :

- “L’unité est ce selon quoi chacune des choses existentes est dite une
- Un nombre est un assemblage composé d’unité,
- Un nombre est une partie d’un nombre, le plus petit du plus grand, lorsque le plus petit mesure le plus grand,
- Le nombre premier est celui qui est mesuré par l’unité seul,
- Le nombre composé est celui qui est mesuré par quelques nombres.”

Il faut bien avoir en tête que l'idée du nombre dans l'antiquité est essentiellement de nature géométrique. Ainsi un nombre A est mesuré ($=$ divisible) par un nombre B si l'on peut faire tenir A un certain nombre entier de fois dans B. Par exemple 4 mesure 12 car en déplaçant 3 fois une règle de longueur 4, on arrivera au bout d'une règle de longueur 12.

Il faut bien avoir en tête que l'idée du nombre dans l'antiquité est essentiellement de nature géométrique. Ainsi un nombre A est mesuré (= divisible) par un nombre B si l'on peut faire tenir A un certain nombre entier de fois dans B. Par exemple 4 mesure 12 car en déplaçant 3 fois une règle de longueur 4, on arrivera au bout d'une règle de longueur 12.

Ce faisant, Euclide décrit la notion de divisibililté (division euclidienne) et définit pour la première fois la notion de nombres premiers.

Il faut bien avoir en tête que l'idée du nombre dans l'antiquité est essentiellement de nature géométrique. Ainsi un nombre A est mesuré (= divisible) par un nombre B si l'on peut faire tenir A un certain nombre entier de fois dans B. Par exemple 4 mesure 12 car en déplaçant 3 fois une règle de longueur 4, on arrivera au bout d'une règle de longueur 12.

Ce faisant, Euclide décrit la notion de divisibililté (division euclidienne) et définit pour la première fois la notion de nombres premiers.

Cette notion géométrique se retrouve par exemple pour la notion de “nombres premiers entre eux”. Pour Euclide, deux nombres entiers a et b sont premiers entre eux s’ils n’ont pas de commune mesure autre que l’unité

Cette notion géométrique se retrouve par exemple pour la notion de “nombres premiers entre eux”. Pour Euclide, deux nombres entiers a et b sont premiers entre eux s’ils n’ont pas de commune mesure autre que l’unité c’est à dire si on soustrait le plus petit au plus grand et qu’on recommence avec les nombres obtenus, on trouve 1.

Cette notion géométrique se retrouve par exemple pour la notion de "nombres premiers entre eux". Pour Euclide, deux nombres entiers a et b sont premiers entre eux s'ils n'ont pas de commune mesure autre que l'unité c'est à dire si on soustrait le plus petit au plus grand et qu'on recommence avec les nombres obtenus, on trouve 1.
C'est exactement l'algorithme d'Euclide !

Cette notion géométrique se retrouve par exemple pour la notion de "nombres premiers entre eux". Pour Euclide, deux nombres entiers a et b sont premiers entre eux s'ils n'ont pas de commune mesure autre que l'unité c'est à dire si on soustrait le plus petit au plus grand et qu'on recommence avec les nombres obtenus, on trouve 1.
C'est exactement l'algorithme d'Euclide ! et le théorème de caractérisation des nombres premiers qui dit que a et b sont premiers entre eux ssi il existe u et v (entiers relatifs) tels que

$$au + bv = 1$$

Cette notion géométrique se retrouve par exemple pour la notion de "nombres premiers entre eux". Pour Euclide, deux nombres entiers a et b sont premiers entre eux s'ils n'ont pas de commune mesure autre que l'unité c'est à dire si on soustrait le plus petit au plus grand et qu'on recommence avec les nombres obtenus, on trouve 1.
C'est exactement l'algorithme d'Euclide ! et le théorème de caractérisation des nombres premiers qui dit que a et b sont premiers entre eux ssi il existe u et v (entiers relatifs) tels que

$$au + bv = 1$$

Euclide prouvera ensuite .... l'infinité des nombres premiers.

Théorème (Euclide)

Il existe une infinité de nombres premiers.

Démonstration:

On raisonne par l'absurde c'est à dire qu'on suppose que le théorème est faux et on en déduit quelque chose d'absurde. Ceci prouve que le théorème ne peut être que vrai.

Théorème (Euclide)

Il existe une infinité de nombres premiers.

Démonstration:

On raisonne par l'absurde c'est à dire qu'on suppose que le théorème est faux et on en déduit quelque chose d'absurde. Ceci prouve que le théorème ne peut être que vrai.

On suppose qu'on a donc un nombre fini de nombres premiers et on en fait une liste : $p_1, p_2, ..., p_n$. On considère le nombre $P = p_1 p_2 ... p_n + 1$. Ce nombre ne peut pas être premier puisqu'il n'est pas dans notre liste. Si il n'est pas premier, il est donc divisible par un des nombres premiers ce qui n'est clairement pas possible E/p_1, E/p_2 .... n'étant pas des nombres entiers. On aboutit bien à une absurdité !

Un peu plus tard, le mathématicien grec Eratostène (200 ans avant J-C) donnera une méthode élégante pour déterminer tous les nombres premiers entre 1 et n (n étant quelconque). C'est le crible d'Eratostène.

Un peu plus tard, le mathématicien grec Eratostène (200 ans avant J-C) donnera une méthode élégante pour déterminer tous les nombres premiers entre 1 et n (n étant quelconque). C'est le crible d'Eratostène.

"J'écris successivement tous les impairs à partir de 3, en une rangée aussi longue que possible, et, en commençant par le premier, j'examine quels sont ceux qu'ils peuvent mesurer. Je trouve qu'il peut mesurer ceux qu'on obtient en passant deux nombres intermédiaires, aussi loin que nous voudrons avancer.
Puis, après cela, prenant un autre point de départ, je considère le deuxième et j'examine quels sont les nombres qu'il peut mesurer; et je trouve que ce sont tous ceux que l'on atteint en passant à chaque fois un groupe de quatre nombres. Recommençons encore une fois ..."

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

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

- On élimine 1.

En langage un peu plus moderne, 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 un peu plus moderne, 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 un peu plus moderne, 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 un peu plus moderne, 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'à la partie entière de la racine de n.

En langage un peu plus moderne, 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'à la partie entière de la racine de 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

	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	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	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			
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 !

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 !

Il est à noter que les sciences chinoises, indiennes, syriennes étaient relativement avancées sur ce sujet.

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 !

Il est à noter que les sciences chinoises, indiennes, syriennes étaient relativement avancées sur ce sujet.
Cependant peu d'avancées significatives vont voir le jour jusqu'au XVIIème siècle.

III. DE EULER A GAUSS

C'est un ecclésiastique français, Marin Mersenne (1588-1648) qui apporte un souffle nouveau à la recherche sur les nombres premiers. Il étudie une famille de nombres aujourd'hui appelé "nombre de Mersenne" qui sont les nombres de la forme :

$$M_p = 2^p - 1$$

Il affirme que ces nombres sont premiers pour :

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

Des oublis dans cette liste seront plus tard évoqués et en 1903, un mathématicien américain Franck Nelson Cole montre ainsi que :

$$2^{67} - 1 = 147573952589676412927 = 193707721 \times 761838257287$$

Aujourd'hui encore ce sont ces nombres qui sont utilisés pour trouver de nouveaux nombres premiers (voir le troisième cours pour l'intérêt de trouver de tels nombres). C'est $2^{32582657} - 1$ (il s'agit du 44ème nombre premier de Mersenne annoncé le 4 septembre 2006 grâce aux efforts d'une collaboration qui porte le nom de GIMPS).

Aujourd'hui encore ce sont ces nombres qui sont utilisés pour trouver de nouveaux nombres premiers (voir le troisième cours pour l'intérêt de trouver de tels nombres). C'est $2^{32582657} - 1$ (il s'agit du 44ème nombre premier de Mersenne annoncé le 4 septembre 2006 grâce aux efforts d'une collaboration qui porte le nom de GIMPS).
On ignore encore si il existe une infinité de nombres de Mersenne premiers.
D'autres mathématiciens se pencheront alors sur ces problèmes (Fermat, Pascal, Goldbach etc...)

Euler (1707-1783) est un des plus grands mathématiciens de tous les temps (surnommé le prince des mathématiciens). Il découvre :

- La théorie des fractions continus

Euler (1707-1783) est un des plus grands mathématiciens de tous les temps (surnommé le prince des mathématiciens). Il découvre :

- La théorie des fractions continus
- Démontre et généralise le petit théorème de Fermat (cf 3ème cours)

Euler (1707-1783) est un des plus grands mathématiciens de tous les temps (surnommé le prince des mathématiciens). Il découvre :

- La théorie des fractions continus
- Démontre et généralise le petit théorème de Fermat (cf 3ème cours)
- fait considérablement progresser l'analyse etc ...

Euler (1707-1783) est un des plus grands mathématiciens de tous les temps (surnommé le prince des mathématiciens). Il découvre :

- La théorie des fractions continus
- Démontre et généralise le petit théorème de Fermat (cf 3ème cours)
- fait considérablement progresser l'analyse etc ...

Il s'interessera également aux nombres premiers. Passionné de démonstration, il était également un calculateur exceptionnel : il produisit par exemple des tables de nombres premiers jusquà 100000 ! Concernant les nombres de Mersenne, il prouve par exemple que

- 431 est un diviseur de $M_{43} = 2^{43} - 1$,
- 1103 divise M_{29}
- 641 divise $2^{2^5} + 1$

Euler (1707-1783) est un des plus grands mathématiciens de tous les temps (surnommé le prince des mathématiciens). Il découvre :

- La théorie des fractions continus
- Démontre et généralise le petit théorème de Fermat (cf 3ème cours)
- fait considérablement progresser l'analyse etc ...

Il s'interessera également aux nombres premiers. Passionné de démonstration, il était également un calculateur exceptionnel : il produisit par exemple des tables de nombres premiers jusquà 100000 ! Concernant les nombres de Mersenne, il prouve par exemple que

- 431 est un diviseur de $M_{43} = 2^{43} - 1$,
- 1103 divise M_{29}
- 641 divise $2^{2^5} + 1$

Cette derniere observation établit la fausseté d'une conjecture de Fermat "Tout nombre de la forme $2^{2^n} + 1$ est premier".

Cette derniere observation établit la fausseté d'une conjecture de Fermat "Tout nombre de la forme $2^{2^n} + 1$ est premier".
Ce résultat montra la difficulté d'obtenir une formule simple engendrant des nombres premiers. Euler écrira :

"Certains mystères échapperont toujours à l'esprit humain. Pour nous en convaincre, il suffit de jeter un oeil aux tableaux des nombres premiers, et l'on verra qu'il n'y règne ni ordre ni règle."

Cette derniere observation établit la fausseté d'une conjecture de Fermat "Tout nombre de la forme $2^{2^n}+1$ est premier".
Ce résultat montra la difficulté d'obtenir une formule simple engendrant des nombres premiers. Euler écrira :

"Certains mystères échapperont toujours à l'esprit humain. Pour nous en convaincre, il suffit de jeter un oeil aux tableaux des nombres premiers, et l'on verra qu'il n'y règne ni ordre ni règle."

Concernant Euler, Gauss a écrit

"Les beautés particulières de ces domaines ont attiré tous ceux qui y ont eu quelque activité; mais nul ne l'a exprimé plus souvent qu'Euler qui, dans presque chacun de ses nombreux articles sur la théorie des nombres, redit à l'envie le plaisir que lui procurent ces investigations, le changement bienvenu qu'elles représentent par rapport aux tâches plus immédiatement liées aux applications pratiques".

Un siècle après la naissance d'Euler suit au autre génie des mathématiques : Carl Friedrich Gauss (1777-1855).

Un siècle après la naissance d'Euler suit au autre génie des mathématiques : Carl Friedrich Gauss (1777-1855).
Tres précoce, il est vite repéré par le duc de Brünswick qui finance ses études. Il travaillera ensuite à Göttingen en Basse Saxe.

Un siècle après la naissance d'Euler suit au autre génie des mathématiques : Carl Friedrich Gauss (1777-1855).
Tres précoce, il est vite repéré par le duc de Brünswick qui finance ses études. Il travaillera ensuite à Göttingen en Basse Saxe.
A l'age de 15 ans (!), il étudie les tables connus de nombres premiers et il découvre de nombreuses erreurs ...à l'age de 18 ans, il réussit à dessiner un polygône régulier à 17 cotés uniquement à la règle et au compas, à 22 ans, il soutient une thèse où figure la première démonstration rigoureuse du théorème :

"Un polynôme de degré n possède exactement n racines dans $\mathbb{C}$ comptées avec multiplicité"

Il est aussi à l'origine de

- la théorie des congruences (cf prochain cours et cours de théorie des groupes !) dans ses "Disquitiones Arethmeticae" (1801).

Il est aussi à l'origine de

- la théorie des congruences (cf prochain cours et cours de théorie des groupes !) dans ses "Disquitiones Arethmeticae" (1801).
- des avancés majeurs en probabilités (loi de Laplace-Gauss)

Il est aussi à l'origine de

- la théorie des congruences (cf prochain cours et cours de théorie des groupes !) dans ses "Disquitiones Arethmeticae" (1801).
- des avancés majeurs en probabilités (loi de Laplace-Gauss)
- d'avancées en géométrie mais aussi en Astronomie, Sc Physiques etc ...

Il est aussi à l'origine de

- la théorie des congruences (cf prochain cours et cours de théorie des groupes !) dans ses "Disquitiones Arethmeticae" (1801).
- des avancés majeurs en probabilités (loi de Laplace-Gauss)
- d'avancées en géométrie mais aussi en Astronomie, Sc Physiques etc ...

Citons aussi le

Théorème (de Gauss)

Si a, b et c sont des nombres entiers, si a divise le produit bc et si a est premier avec b alors a divise c.

Il est aussi à l'origine de

- la théorie des congruences (cf prochain cours et cours de théorie des groupes !) dans ses "Disquitiones Arethmeticae" (1801).
- des avancés majeurs en probabilités (loi de Laplace-Gauss)
- d'avancées en géométrie mais aussi en Astronomie, Sc Physiques etc ...

Citons aussi le

Théorème (de Gauss)

Si a, b et c sont des nombres entiers, si a divise le produit bc et si a est premier avec b alors a divise c.

Ce théorème permet de donner une démonstration aisée du :

Théorème (fondamental de l'arithmétique)

Tout nombre entier positif se décompose de manière unique en produit de nombres premiers.

La partie existence est évidente par récurrence et la partie unicité découle du théorème de Gauss.

Théorème (fondamental de l'arithmétique)

Tout nombre entier positif se décompose de manière unique en produit de nombres premiers.

La partie existence est évidente par récurrence et la partie unicité découle du théorème de Gauss.

Concernant nos problèmes, Gauss s'interesse à la répartition des nombres premiers. Mais le problème est attaqué de façon différente ici.

Au lien de se demander :

"Quel est l'emplacement exact des nombres premiers dans une table de nombres ?"

Il pose le problème :

"Peut-on estimer combien de nombres premiers on a entre 1 et un nombre N quelconque ?"

Au lien de se demander :

"Quel est l'emplacement exact des nombres premiers dans une table de nombres ?"

Il pose le problème :

"Peut-on estimer combien de nombres premiers on a entre 1 et un nombre N quelconque ?"

Par exemple, il y a 25 nombres premiers compris entre 1 et 100, ie 1 nombre compris entre 1 est 100 sur 4 est premier, comment cette quantité se modifie pour les nombres de 1 à 1000 ? 1 à 10000 ? etc ...

Au lien de se demander :

"Quel est l'emplacement exact des nombres premiers dans une table de nombres ?"

Il pose le problème :

"Peut-on estimer combien de nombres premiers on a entre 1 et un nombre N quelconque ?"

Par exemple, il y a 25 nombres premiers compris entre 1 et 100, ie 1 nombre compris entre 1 est 100 sur 4 est premier, comment cette quantité se modifie pour les nombres de 1 à 1000 ? 1 à 10000 ? etc ...

Soit $\Pi(N)$ le nombre de premier entre 1 et N. En quoi connaître Π permet de trouver tous les nombres premiers ?

Au lien de se demander :

"Quel est l'emplacement exact des nombres premiers dans une table de nombres ?"

Il pose le problème :

"Peut-on estimer combien de nombres premiers on a entre 1 et un nombre N quelconque ?"

Par exemple, il y a 25 nombres premiers compris entre 1 et 100, ie 1 nombre compris entre 1 est 100 sur 4 est premier, comment cette quantité se modifie pour les nombres de 1 à 1000 ? 1 à 10000 ? etc ...

Soit $\Pi(N)$ le nombre de premier entre 1 et N. En quoi connaître Π permet de trouver tous les nombres premiers ?

$$\Pi(N+1) = \Pi(N) + 1 \iff N+1 \text{ est premier}$$

Table tirée du livre de Marcus de Sautoy (cf. reférence)

Nombre entier N	Repartition des nombres premiers (environ)
10	1 sur 2,5
100	1 sur 4
1000	1 sur 6
10.000	1 sur 8,1
1.000.000	1 sur 12,7
1.000.000.000	1 sur 19,7

Table tirée du livre de Marcus de Sautoy (cf. reférence).

Nombre entier N	Repartition des nombres premiers (environ)	ln N
10	1 sur 2,5	2,3
100	1 sur 4	4,6
1000	1 sur 6	6,9
10.000	1 sur 8,1	9,2
1.000.000	1 sur 12,7	13,8
1.000.000.000	1 sur 19,7	20,7

Table tirée du livre de Marcus de Sautoy (cf. reférence).

Nombre entier N	Repartition des nombres premiers (environ)	ln N
10	1 sur 2,5	2,3
100	1 sur 4	4,6
1000	1 sur 6	6,9
10.000	1 sur 8,1	9,2
1.000.000	1 sur 12,7	13,8
1.000.000.000	1 sur 19,7	20,7

Une estimation donnée par Gauss est donc que le nombre de nombres premiers entre 1 et N est voisin de $N/ln(N)$.

Cette découverte (rapport entre $\Pi(N)$ et logarithme) pourtant fondamental n'a jamais été annoncée publiquement par Gauss, réticent à l'idée de dévoiler une idée sans démonstrations.

Cette découverte (rapport entre $\Pi(N)$ et logarithme) pourtant fondamental n'a jamais été annoncée publiquement par Gauss, réticent à l'idée de dévoiler une idée sans démonstrations.
C'est d'ailleurs une des grands caractéristique de Gauss : mettre l'accent sur la rigueur, la valeur de démonstration en Mathématiques ce qui influencera les mathématiques par la suite (et qui différentiera cette science des autres disciplines scientifiques).

Cette découverte (rapport entre $\Pi(N)$ et logarithme) pourtant fondamental n'a jamais été annoncée publiquement par Gauss, réticent à l'idée de dévoiler une idée sans démonstrations.
C'est d'ailleurs une des grands caractéristique de Gauss : mettre l'accent sur la rigueur, la valeur de démonstration en Mathématiques ce qui influencera les mathématiques par la suite (et qui différentiera cette science des autres disciplines scientifiques).
Ce rapport entre logarithme et répartition des nombres premiers sera rendu public par Legendre (1752-1833, grand mathématicien français en conflit permanent avec Gauss durant toute sa vie). Il affinera meme la prévision de Gauss en remplaçant $N/\ln(N)$ par :

$$\frac{N}{\ln(N) - 1,08366}$$

Cette découverte (rapport entre $\Pi(N)$ et logarithme) pourtant fondamental n'a jamais été annoncée publiquement par Gauss, réticent à l'idée de dévoiler une idée sans démonstrations.
C'est d'ailleurs une des grands caractéristique de Gauss : mettre l'accent sur la rigueur, la valeur de démonstration en Mathématiques ce qui influencera les mathématiques par la suite (et qui différentiera cette science des autres disciplines scientifiques).
Ce rapport entre logarithme et répartition des nombres premiers sera rendu public par Legendre (1752-1833, grand mathématicien français en conflit permanent avec Gauss durant toute sa vie). Il affinera meme la prévision de Gauss en remplaçant $N/\ln(N)$ par :

$$\frac{N}{\ln(N) - 1,08366}$$

Ce n'est qu'après sa mort qu'on se rendit compte que c'est Gauss qui avait déterminé ce rapport logarithme-répartition des nombres premiers ... le premier !

Ce n'est qu'après sa mort qu'on se rendit compte que c'est Gauss qui avait déterminé ce rapport logarithme-répartition des nombres premiers ... le premier !

En fait, Gauss fit beaucoup mieux : à partir d'observations statistiques, il en vient à conjecturer que le nombre $\pi(N)$ de nombres premiers entre 1 et N est proche de :

$$\mathrm{Li}(N) = \int_{j=2}^{N} \frac{du}{\ln(u)}$$

Ce n'est qu'après sa mort qu'on se rendit compte que c'est Gauss qui avait déterminé ce rapport logarithme-répartition des nombres premiers ... le premier !

En fait, Gauss fit beaucoup mieux : à partir d'observations statistiques, il en vient à conjecturer que le nombre $\pi(N)$ de nombres premiers entre 1 et N est proche de :

$$\mathrm{Li}(N) = \int_{j=2}^{N} \frac{du}{\ln(u)}$$

A la fin de sa vie, Gauss admit avoir construit des tables de nombres premiers jusqu'à 3.000.000 !!!

"Bien souvent, j'ai profité d'un quart d'heure d'oisiveté pour me livrer ça et là au décompte d'une chiliade (un intervalle de 1000 nombres) supplémentaires".

A cette date, tout ceci ne reste que des observations mysterieuses mais celles-ci insufflent un nouveau souffle dans le domaine de la recherche sur les nombres premiers.

A cette date, tout ceci ne reste que des observations mysterieuses mais celles-ci insufflent un nouveau souffle dans le domaine de la recherche sur les nombres premiers.
La conjecture de Gauss-Legendre nous dit donc la chose suivante :

$$\lim_{N\to\infty} \frac{\Pi(N)}{\frac{N}{\ln(N)}} = 1.$$

C'est en fait un théorème, dit "théorème des nombres premiers" prouvé par Vallée Poussin et Hadamard en ... 1896 soit 50 ans plus tard.

Il existe maintenant de nombreuses différentes démonstrations de ce théorème mais aucune n'est vraiment simple. Certaines demandent un bagage mathématiques important. D'autres n'utilisent que des mathématiques rudimentaires mais sont longues et laborieuses.

Il existe maintenant de nombreuses différentes démonstrations de ce théorème mais aucune n'est vraiment simple. Certaines demandent un bagage mathématiques important. D'autres n'utilisent que des mathématiques rudimentaires mais sont longues et laborieuses.

Le principe de la démonstration de Vallée Poussin et Hadamard est d'appliquer les idées d'un étudiant de Gauss : Riemann qui va révolutionner la recherche en théorie des nombres mais aussi les Mathématiques dans leur ensemble.