Histoire des nombres premiers

$3^{\text{ème}}$ partie : Récentes découvertes et applications

N. Jacon

Université de Franche-Comté

I. CRYPTOGRAPHIE

1-Un peu de Mathématiques : la calculatrice horloge de Gauss

En 1801, Gauss invente un outil fondamental qui facilite grandement les raisonnements arithmétiques : l'arithmétique modulaire.

La calculatrice horloge se réfère à l'addition des heures indiquées par la petite aiguille d'une horloge :

1-Un peu de Mathématiques : la calculatrice horloge de Gauss

En 1801, Gauss invente un outil fondamental qui facilite grandement les raisonnements arithmétiques : l'arithmétique modulaire.

La calculatrice horloge se réfère à l'addition des heures indiquées par la petite aiguille d'une horloge :

Ainsi, si on commence à 2 heures et si on ajoute 11 heures, alors plutôt que d'arriver à 13 heures comme dans l'addition classique, on arrive à 1 heure. De même, si on commence à 0 heure et qu'on attend 7 heures 4 fois de suite, on arrive à

1-Un peu de Mathématiques : la calculatrice horloge de Gauss

En 1801, Gauss invente un outil fondamental qui facilite grandement les raisonnements arithmétiques : l'arithmétique modulaire.

La calculatrice horloge se réfère à l'addition des heures indiquées par la petite aiguille d'une horloge :

Ainsi, si on commence à 2 heures et si on ajoute 11 heures, alors plutôt que d'arriver à 13 heures comme dans l'addition classique, on arrive à 1 heure. De même, si on commence à 0 heure et qu'on attend 7 heures 4 fois de suite, on arrive à 4 (au lieu de 28).

En fait, quand on arrive à 12, on recommence à zéro; on dit qu'on travaille modulo 12. Pour reprendre l'exemple précédent, on dit que 28 et 4 sont congrus modulo 12 et on note $28 \equiv 4 (\mathrm{mod}\ 12)$. Les nombres 4 ; 16 ; 28 ; 40 ; etc sont considérés comme égaux lorsqu'on travaille modulo 12.

En fait, quand on arrive à 12, on recommence à zéro; on dit qu'on travaille modulo 12. Pour reprendre l'exemple précédent, on dit que 28 et 4 sont congrus modulo 12 et on note $28 \equiv 4 (\mathrm{mod}\ 12)$. Les nombres 4 ; 16 ; 28 ; 40 ; etc sont considérés comme égaux lorsqu'on travaille modulo 12.

Pour généraliser, on peut évidemment penser à une horloge qui contient n heures, et faire des calculs avec modulo n.

En fait, quand on arrive à 12, on recommence à zéro; on dit qu'on travaille modulo 12. Pour reprendre l'exemple précédent, on dit que 28 et 4 sont congrus modulo 12 et on note $28 \equiv 4 (\mathrm{mod}\ 12)$. Les nombres 4 ; 16 ; 28 ; 40 ; etc sont considérés comme égaux lorsqu'on travaille modulo 12.

Pour généraliser, on peut évidemment penser à une horloge qui contient n heures, et faire des calculs avec modulo n.

L'ensemble considéré ici est constitué d'éléments $\{0, 1, ..., n-1\}$ et il est muni d'une loi d'addition définie ci-dessus qui en fait un groupe et appelée groupe cyclique.

Travailler avec l'arithmétique modulaire ce n'est rien d'autre que faire de la division euclidienne ainsi $a \equiv r (\mathrm{mod}\ n)$ pour un nombre $r \in \{0, 1, ..., n-1\}$ si et seulement si le reste de la division euclidienne de a par n est r.

Travailler avec l'arithmétique modulaire ce n'est rien d'autre que faire de la division euclidienne ainsi $a \equiv r (\mathrm{mod}\ n)$ pour un nombre $r \in \{0, 1, ..., n-1\}$ si et seulement si le reste de la division euclidienne de a par n est r.

Mais c'est trés pratique ! par exemple comment savoir quel est le reste de la division euclidienne de 100^{1000} par 9 ?

Travailler avec l'arithmétique modulaire ce n'est rien d'autre que faire de la division euclidienne ainsi $a \equiv r(\mathrm{mod}\ n)$ pour un nombre $r \in \{0, 1, ..., n-1\}$ si et seulement si le reste de la division euclidienne de a par n est r.

Mais c'est trés pratique ! par exemple comment savoir quel est le reste de la division euclidienne de 100^{1000} par 9 ?

On a $100 \equiv 1(\mathrm{mod}\ 9)$ donc $100^{1000} \equiv 1(\mathrm{mod}\ 9)$ et le reste de cette division euclidienne est donc 1.

Les groupes cycliques sont une classe importante de groupes (cf - l'excellent - cours de l'année prochaine). Il sont commutatifs et lorsqu'ils sont constitués de p éléments avec p premier, ils sont même des corps !

Dans ce cas, ils font aussi partis de la classification des groupes finis simples.

Théorème (Petit théorème de Fermat)

Si p est un nombre premier, alors pour tout entier a,

$$a^p \equiv a (mod\ p)$$

1-La cryptographie à clef publique

Dans la deuxième moitié du XXème siècle, des découvertes fondamentales vont sucitées un intérêt considérable sur les nombres premiers. Ces découvertes, liées à la cryptographie ont maintenant acquis une grande importance économique.

1-La cryptographie à clef publique

Dans la deuxième moitié du XXème siècle, des découvertes fondamentales vont sucitées un intérêt considérable sur les nombres premiers. Ces découvertes, liées à la cryptographie ont maintenant acquis une grande importance économique.

La cryptographie correspond à l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique.

1-La cryptographie à clef publique

Dans la deuxième moitié du XXème siècle, des découvertes fondamentales vont sucitées un intérêt considérable sur les nombres premiers. Ces découvertes, liées à la cryptographie ont maintenant acquis une grande importance économique.

La cryptographie correspond à l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique.

Elle existait depuis longtemps déjà (Enigma ...) mais un article de mathématiciens de Stanford de 1976 va révolutionner le concept. Il propose la *cryptographie à clef publique*. Celle-ci sera en particulier très bien adaptée aux nouveaux défis de codage induit par Internet, les téléphones portables etc ...

Le principe est le suivant : une banque veut obtenir le numéro de carte bancaire de son client. Pour cela, elle construit deux clefs :

- La première est publique et est communiquée au client.

Le principe est le suivant : une banque veut obtenir le numéro de carte bancaire de son client. Pour cela, elle construit deux clefs :

- La première est publique et est communiquée au client.
- La deuxième est privée et reste en la possession de la banque.

Le principe est le suivant : une banque veut obtenir le numéro de carte bancaire de son client. Pour cela, elle construit deux clefs :

- La première est publique et est communiquée au client.
- La deuxième est privée et reste en la possession de la banque.

La clef publique sert à coder : le client peut coder le numéro de carte grâce à cette clef et l'envoyer à la banque.

Le principe est le suivant : une banque veut obtenir le numéro de carte bancaire de son client. Pour cela, elle construit deux clefs :

- La première est publique et est communiquée au client.
- La deuxième est privée et reste en la possession de la banque.

La clef publique sert à coder : le client peut coder le numéro de carte grâce à cette clef et l'envoyer à la banque.
La clef privée sert à décoder : la banque retrouve le numéro de carte grâce à celle-ci

Le principe est le suivant : une banque veut obtenir le numéro de carte bancaire de son client. Pour cela, elle construit deux clefs :

- La première est publique et est communiquée au client.
- La deuxième est privée et reste en la possession de la banque.

La clef publique sert à coder : le client peut coder le numéro de carte grâce à cette clef et l'envoyer à la banque.
La clef privée sert à décoder : la banque retrouve le numéro de carte grâce à celle-ci

Avantage : la banque et le client n'ont plus besoin de se rencontrer pour convenir d'un code de dechiffrage secret, aucune information capitale de déchiffrage ne circule entre les deux interlocuteurs !

3-Le modèle de cryptographie RSA

La question était maintenant de savoir si un système concret de cryptographie à clef publique pouvait être construit.

3-Le modèle de cryptographie RSA

La question était maintenant de savoir si un système concret de cryptographie à clef publique pouvait être construit.
Un tel système va être proposé par 3 mathématiciens du MIT de Boston (USA) grâce à la théorie des nombres : Rivest, Shamir et Adleman.

3-Le modèle de cryptographie RSA

La question était maintenant de savoir si un système concret de cryptographie à clef publique pouvait être construit.
Un tel système va être proposé par 3 mathématiciens du MIT de Boston (USA) grâce à la théorie des nombres : Rivest, Shamir et Adleman.
Ce système est devenu un système universel utilisé par les principaux groupes informatiques, intégré dans les cartes Ethernet, dans certaines cartes à puces bancaires, dans les couriers élèctroniques etc ...

Le système RSA repose sur le théorème suivant :

Théorème

Soient p et q deux nombres premiers. On pose $n = pq$. Si e est un entier premier avec $(p-1)(q-1)$ alors il existe un entier $d > 0$ tel que :

$$ed \equiv 1 \ (mod \ (p-1)(q-1))$$

Pour cet entier d et pour un entier a quelconque, on a :

$$a^{ed} \equiv a (mod \ n)$$

SITUATION : Un client veut faire parvenir son numero de carte bancaire C à une banque ...

SITUATION : Un client veut faire parvenir son numero de carte bancaire C à une banque ... un pirate veut l'obtenir.

SITUATION : Un client veut faire parvenir son numero de carte bancaire C à une banque ... un pirate veut l'obtenir.

$1^{\text{ère}}$ Etape : La banque choisit les données suivantes :

- Deux nombres premiers p et q,

SITUATION : Un client veut faire parvenir son numero de carte bancaire C à une banque ... un pirate veut l'obtenir.

$1^{\text{ère}}$ Etape : La banque choisit les données suivantes :

- Deux nombres premiers p et q,
- Un entier e premier avec $(p-1)(q-1)$ (facile à trouver),

SITUATION : Un client veut faire parvenir son numero de carte bancaire C à une banque ... un pirate veut l'obtenir.

$1^{\text{ère}}$ Etape : La banque choisit les données suivantes :

- Deux nombres premiers p et q,
- Un entier e premier avec $(p-1)(q-1)$ (facile à trouver),
- Un entier d vérifiant les données de l'énoncé du théorème c'est à dire tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$ (facile à trouver).

SITUATION : Un client veut faire parvenir son numero de carte bancaire C à une banque ... un pirate veut l'obtenir.

1ère Etape : La banque choisit les données suivantes :

- Deux nombres premiers p et q,
- Un entier e premier avec $(p-1)(q-1)$ (facile à trouver),
- Un entier d vérifiant les données de l'énoncé du théorème c'est à dire tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$ (facile à trouver).

2ème Etape : La banque rend publique le nombre $n = pq$ (qui doit être plus grand que les numéros à coder) et le nombre e en les communicant aux clients.

$3^{\text{ème}}$ Etape : Le client calcule le nombre $D \equiv C^e \pmod{n}$ et envoie ce nombre à la banque.

$3^{\text{ème}}$ Etape : Le client calcule le nombre $D \equiv C^e \pmod{n}$ et envoie ce nombre à la banque.

A ce stade, Le pirate peut disposer des nombres n (qui est égale à pq), du nombre e et de ce nombre $D = C^e \pmod{n}$.

$3^{\text{ème}}$ Etape : Le client calcule le nombre $D \equiv C^e \pmod{n}$ et envoie ce nombre à la banque.

A ce stade, Le pirate peut disposer des nombres n (qui est égale à pq), du nombre e et de ce nombre $D = C^e \pmod{n}$.

$4^{\text{ème}}$ Etape : La banque qui veut avoir C n'a plus qu'à calculer $D^d \pmod{n}$ qui est égale à C d'après le théorème ci-dessus.

$3^{\text{ème}}$ Etape : Le client calcule le nombre $D \equiv C^e \pmod{n}$ et envoie ce nombre à la banque.

A ce stade, Le pirate peut disposer des nombres n (qui est égale à pq), du nombre e et de ce nombre $D = C^e \pmod{n}$.

$4^{\text{ème}}$ Etape : La banque qui veut avoir C n'a plus qu'à calculer $D^d \pmod{n}$ qui est égale à C d'après le théorème ci-dessus.

Pour le Pirate, la seule manière efficace de trouver C est d'effectuer le même calcul. Pour ceci, il doit déterminer d. Le seul moyen d'y parvenir est de disposer des nombres premiers p et q. Son problème se résume donc à :

Etant donné $n = pq$, déterminer p et q

UN EXEMPLE

La banque choisit les données suivantes :

- Deux nombres premiers $p = 31$ et $q = 7$,

UN EXEMPLE

La banque choisit les données suivantes :

- Deux nombres premiers $p = 31$ et $q = 7$,
- Un entier e premier avec $(p-1)(q-1)$: $e = 7$ par exemple,

UN EXEMPLE

La banque choisit les données suivantes :

- Deux nombres premiers $p = 31$ et $q = 7$,
- Un entier e premier avec $(p-1)(q-1)$: $e = 7$ par exemple,
- Un entier d vérifiant les données de l'énoncé du théorème c'est à dire tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$. On trouve $d = 103$.

UN EXEMPLE

La banque choisit les données suivantes :

- Deux nombres premiers $p = 31$ et $q = 7$,
- Un entier e premier avec $(p-1)(q-1)$: $e = 7$ par exemple,
- Un entier d vérifiant les données de l'énoncé du théorème c'est à dire tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$. On trouve $d = 103$.

La banque rend publique le nombres $n = pq = 217$ et le nombre $e = 7$ en les communicant aux clients.

UN EXEMPLE

La banque choisit les données suivantes :

- Deux nombres premiers $p = 31$ et $q = 7$,
- Un entier e premier avec $(p-1)(q-1)$: $e = 7$ par exemple,
- Un entier d vérifiant les données de l'énoncé du théorème c'est à dire tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$. On trouve $d = 103$.

La banque rend publique le nombres $n = pq = 217$ et le nombre $e = 7$ en les communicant aux clients.
Le numéro de carte du client est $C = 113$ (qui doit etre plus petit que n). Le client calcule alors $113^7 \pmod{217}$. Il trouve $D = 204$: c'est le numéro codé qu'il envoie à la banque.

UN EXEMPLE

La banque choisit les données suivantes :

- Deux nombres premiers $p = 31$ et $q = 7$,
- Un entier e premier avec $(p-1)(q-1)$: $e = 7$ par exemple,
- Un entier d vérifiant les données de l'énoncé du théorème c'est à dire tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$. On trouve $d = 103$.

La banque rend publique le nombres $n = pq = 217$ et le nombre $e = 7$ en les communicant aux clients.
Le numéro de carte du client est $C = 113$ (qui doit etre plus petit que n). Le client calcule alors $113^7 \pmod{217}$. Il trouve $D = 204$: c'est le numéro codé qu'il envoie à la banque. Pour décoder, la banque calcule $D^d \pmod{217}$ qui donne 113.

4. Le problème de factorisation

Pour le pirate, la seule manière de "casser" le code RSA (pour l'instant ...) est de résoudre le problème : étant donné un nombre n produit de deux nombres premiers, trouver ces 2 nombres. En quoi est-ce un problème difficile ?

4. Le problème de factorisation

Pour le pirate, la seule manière de "casser" le code RSA (pour l'instant ...) est de résoudre le problème : étant donné un nombre n produit de deux nombres premiers, trouver ces 2 nombres. En quoi est-ce un problème difficile ?

Déjà, on n'a aucun moyen efficace pour trouver des grands nombres premiers ... mais la confiance en ce système vient surtout du fait que depuis plus de 20 ans, aucun algorithme efficace n'a permis de résoudre ce problème...

4. Le problème de factorisation

Pour le pirate, la seule manière de "casser" le code RSA (pour l'instant ...) est de résoudre le problème : étant donné un nombre n produit de deux nombres premiers, trouver ces 2 nombres. En quoi est-ce un problème difficile ?

Déjà, on n'a aucun moyen efficace pour trouver des grands nombres premiers ... mais la confiance en ce système vient surtout du fait que depuis plus de 20 ans, aucun algorithme efficace n'a permis de résoudre ce problème...

... mais rien ne nous prouve qu'il n'en existe pas un !

4. Le problème de factorisation

Pour le pirate, la seule manière de "casser" le code RSA (pour l'instant ...) est de résoudre le problème : étant donné un nombre n produit de deux nombres premiers, trouver ces 2 nombres. En quoi est-ce un problème difficile ?

Déjà, on n'a aucun moyen efficace pour trouver des grands nombres premiers ... mais la confiance en ce système vient surtout du fait que depuis plus de 20 ans, aucun algorithme efficace n'a permis de résoudre ce problème...

... mais rien ne nous prouve qu'il n'en existe pas un !

Voilà pourquoi certaines sociétés offrent de belles sommes pour trouver de nouveaux nombres premiers.

Pourquoi le “pour l’instant” ?

Pourquoi le “pour l’instant” ? Dan Boneh de Stanford a montré que casser RSA n’est pas équivalent au problème de factorisation.
Enfin, voici un exemple d’algorithme résolvant le problème de facorisation. Soit N un nombre entier et soit p un des facteurs premiers de N qu’on cherche à déterminer. Soit a un entier premier avec N (et donc avec p). Pour un entier k, on a le résultat suivant :

$$\text{Si } (p-1) \text{ divise } k!, \text{ alors } p \text{ divise } a^{k!}-1$$

Pourquoi le “pour l'instant” ? Dan Boneh de Stanford a montré que casser RSA n'est pas équivalent au problème de factorisation.
Enfin, voici un exemple d'algorithme résolvant le problème de facorisation. Soit N un nombre entier et soit p un des facteurs premiers de N qu'on cherche à déterminer. Soit a un entier premier avec N (et donc avec p). Pour un entier k, on a le résultat suivant :

$$\text{Si } (p-1) \text{ divise } k!, \text{ alors } p \text{ divise } a^{k!}-1$$

En effet si $p-1$ divise $k!$ alors $k!$ s'écrit $r(p-1)$ pour $r \geqslant 1$ et alors $a^{k!}-1 = (a^{p-1}-1)(1+a+\ldots+a^r)$ et on conclut avec le petit théorème de Fermat.

Ainsi si p est un nombre premier divisant N tel que $p-1$ divise $k!$ alors p est un nombre premier divisant N et divisant $a^{k!}-1$.

Donc p est un nombre divisant le pgcd de N et $a^{k!}-1 (\mathrm{mod}\ N)$

Si $(p-1)$ est un produit de petit facteur alors on tombe facilement sur un k tel que $(p-1)$ divise $k!$ ... et donc sur un diviseur de N et $a^{k!}-1 (\mathrm{mod}\ N)$. L'algorithme peut alors être efficace (toute proportion gardée).

Il existe maintenant beaucoup de systèmes de cryptographie concurrent au système RSA, certains faisant intervenir d'autres domaines de théorie des nombres (courbes elliptiques) mais ce système et ses dérivées restent néanmoins l'un des plus fiables.

5. Un mot sur les Tests de primalité

Un enjeu important est de déterminer un bon algorithme permettant de savoir si un nombre est premier

5. Un mot sur les Tests de primalité

Un enjeu important est de déterminer un bon algorithme permettant de savoir si un nombre est premier pour pouvoir crypter au mieux mais aussi pour pouvoir décrypter !

On distingue en général deux types de tests :

- Les algorithmes déterministes “surs”,

5. Un mot sur les Tests de primalité

Un enjeu important est de déterminer un bon algorithme permettant de savoir si un nombre est premier pour pouvoir crypter au mieux mais aussi pour pouvoir décrypter !

On distingue en général deux types de tests :

- Les algorithmes déterministes “surs”,
- les algorithmes probabilistes.

La méthode du crible d'Erathostène fournit un test déterministe mais très couteux pour voir si un nombre est premier ou composé

Un des tests probablisites les plus connus utilise le petit théorème de Fermat :

Théorème (Petit théorème de Fermat)

Si p est un nombre premier, alors pour tout entier $a \neq 0$,

$$a^{p-1} \equiv 1(mod\ p)$$

Par contre, $561 = 3 \times 11 \times 17$ n'est pas premier et pour tout entier a premier avec 561, on a pourtant

$$a^{560} \equiv 1 \pmod{561}$$

mais si p est un nombre composé, il est "improbable" que

$$a^p \equiv a(\mathrm{mod}\ p)$$

pour une valeur arbitraire de a.

Par exemple, si

$$1 \equiv 2^{x-1} \equiv 3^{x-1} \equiv 5^{x-1} \equiv 7^{x-1} \pmod{x}$$

alors nous savons que le nombre x est probablement premier.
Le test de primalité de Miller-Rabin et le test de primalité de Solovay-Strassen sont des tests plus compliqués qui utilisent le même type d'idée.

Pour les tests de primalités déterministes, on citera : le test cyclotomique, le test de primalité de courbe elliptique.

Pour les tests de primalités déterministes, on citera : le test cyclotomique, le test de primalité de courbe elliptique.

En 2002, Manindra Agrawal, Nitin Saxena et Neeraj Kayal ont donné un nouveau test déterministe qui s'exécute en temps polynomiale.

Pour les tests de primalités déterministes, on citera : le test cyclotomique, le test de primalité de courbe elliptique.

En 2002, Manindra Agrawal, Nitin Saxena et Neeraj Kayal ont donné un nouveau test déterministe qui s'exécute en temps polynomiale.

La plupart des tests probabilistes peuvent aussi se transformer en tests déterministes.

II. NOMBRES PREMIERS ET CHAOS QUANTIQUES

Revenons à l'hypothèse de Riemann, on se rappelle que celle-ci prédisait ques les zéros non triviaux de la fonction zeta étaient de la forme :

$$\frac{1}{2} + i\gamma$$

Admettons que celle-ci soit vrai. Prenons un réel T, la hauteur. On regarde tous les zéros $\frac{1}{2} + i\gamma$ tels que $0 \leqslant \gamma \leqslant T$.

Revenons à l'hypothèse de Riemann, on se rappelle que celle-ci prédisait ques les zéros non triviaux de la fonction zeta étaient de la forme :

$$\frac{1}{2} + i\gamma$$

Admettons que celle-ci soit vrai. Prenons un réel T, la hauteur. On regarde tous les zéros $\frac{1}{2} + i\gamma$ tels que $0 \leqslant \gamma \leqslant T$.

Une question naturelle est alors de se demander quelle est la répartition de ces nombres sur le segment $[0, T]$?

Conjecture (Montgomery 1973)

Le nombre attendu de zéro dans un intervalle de longueur T multiplié par la longueur moyenne du saut qui suit un zéro est :

$$\int_0^T \left(1 - \left(\frac{sin(\pi u)}{u} du\right)\right)$$

Complètement par hasard, Montgomery se rend compte avec un physicien théoricien Dyson que (en (très) gros) le schéma de répartition des zéros de Riemann semble coincider avec ce que les physiciens tentent de modéliser avec les niveaux d'énergie des atomes lourds ...

Intérêt du point de vue Hypothèse de Riemann ?

Intérêt du point de vue Hypothèse de Riemann ? si ces zéros pouvaient être expliqués en considérant ces niveau d'énergie, on pourrait éventuellement montrer que tous les zéro de Riemann sont sur la "bonne" droite, un zéro à l'extèrieur de cette droite correspondant à un niveau d'énergie impossible.

Intérêt du point de vue Hypothèse de Riemann ? si ces zéros pouvaient être expliqués en considérant ces niveau d'énergie, on pourrait éventuellement montrer que tous les zéro de Riemann sont sur la "bonne" droite, un zéro à l'extèrieur de cette droite correspondant à un niveau d'énergie impossible.

Cet conjecture assez incroyable sembla être confirmée par des calculs-essais d'Odlyko ...

Le chaos quantique désigne un champ de recherches qui est issu des succès de la théorie du chaos. Le problème essentiel de cette théorie est la question suivante : Quel est le comportement en mécanique quantique d'un système classiquement chaotique ?

Le terme chaos est utilisé quand un système dynamique est particulièrement sensible aux conditions de départ.

C'est essentiellement un physicien, Berry, qui comprit que le système dynamique qui semblait lié au paysage de la fonction zéta correspondait à un système chaotique.

Notons que cette observation ne s'arrête pas là : il existe plusieurs type de fonctions zéta et des mathématiciens tel que Sarnak et Rubinstein ont découvert d'excellentes corrélations entre les zéros de ces fonctions et des niveaux d'énergie de divers systèmes chaotiques.

Notons que cette observation ne s'arrête pas là : il existe plusieurs type de fonctions zéta et des mathématiciens tel que Sarnak et Rubinstein ont découvert d'excellentes corrélations entre les zéros de ces fonctions et des niveaux d'énergie de divers systèmes chaotiques.

A. Granville : "Le coté le plus intuitif du chaos quantique permet de faire des prédictions plus fructueuses sur la répartition des nombres premiers. D'autre part, le développement plus prudent de la théorie des nombres premiers conduit à des conjectures plus précises dans le domaine du chaos quantique."

III. CONCLUSION

Quelques questions encore ouvertes :

- La conjecture de Goldbach : tout nombre pair strictement supérieur à 2, peut-il s'écrire comme somme de deux nombres premiers ?

Quelques questions encore ouvertes :

- 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 : Existe-t-il une infinité de jumeaux premiers ?

Quelques questions encore ouvertes :

- 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 : Existe-t-il une infinité de jumeaux premiers ?
- Toute suite de Fibonacci contient-elle une infinité de nombres premiers ?

Quelques questions encore ouvertes :

- 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 : Existe-t-il une infinité de jumeaux premiers ?
- Toute suite de Fibonacci contient-elle une infinité de nombres premiers ?
- Existe-t-il une infinité de nombres premiers de Fermat ?

Quelques questions encore ouvertes :

- 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 : Existe-t-il une infinité de jumeaux premiers ?
- Toute suite de Fibonacci contient-elle une infinité de nombres premiers ?
- Existe-t-il une infinité de nombres premiers de Fermat ?
- Y a-t-il une infinité de nombres premiers de la forme $n^2 + 1$?

Quelques questions encore ouvertes :

- 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 : Existe-t-il une infinité de jumeaux premiers ?
- Toute suite de Fibonacci contient-elle une infinité de nombres premiers ?
- Existe-t-il une infinité de nombres premiers de Fermat ?
- Y a-t-il une infinité de nombres premiers de la forme $n^2 + 1$?
- Y a-t-il une infinité de nombres premiers factoriels ?

Quelques questions encore ouvertes :

- 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 : Existe-t-il une infinité de jumeaux premiers ?
- Toute suite de Fibonacci contient-elle une infinité de nombres premiers ?
- Existe-t-il une infinité de nombres premiers de Fermat ?
- Y a-t-il une infinité de nombres premiers de la forme $n^2 + 1$?
- Y a-t-il une infinité de nombres premiers factoriels ?
- Y a-t-il une infinité de nombres premiers primoriels ?

Quelques questions encore ouvertes :

- 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 : Existe-t-il une infinité de jumeaux premiers ?
- Toute suite de Fibonacci contient-elle une infinité de nombres premiers ?
- Existe-t-il une infinité de nombres premiers de Fermat ?
- Y a-t-il une infinité de nombres premiers de la forme $n^2 + 1$?
- Y a-t-il une infinité de nombres premiers factoriels ?
- Y a-t-il une infinité de nombres premiers primoriels ?

On a vu les applications et les questions que ces nombres posent dans des domaines aussi surpranant que l'informatique ou la physique quantique. Indépendemment, ces nombres sont bien sûr primordiale dans tous les domaines mathématiques (voir l'exemple de l'arithmétique modulaire).

On a vu les applications et les questions que ces nombres posent dans des domaines aussi surpranant que l'informatique ou la physique quantique. Indépendemment, ces nombres sont bien sûr primordiale dans tous les domaines mathématiques (voir l'exemple de l'arithmétique modulaire).

Concernant l'hypothèse de Riemann, vrai ? fausse ? indémontrable ? elle a de toute facon éclairé beaucoup de domaines des mathématiques.

M. De Sautoy “Jusque là, nous écouterons, ensorcelés par cette musique mathématique imprévisible, incapable d’en maîtriser les tours et détours. Les nombres premiers nous ont toujours accompagnés dans notre exploration du monde mathématique, et pourtant, ils restent les plus énigmatiques des nombres. En dépit des meilleurs efforts des plus grands esprits mathématiques afin d’expliquer la modulation et la transformation de cette musique mystique, ils restent un mystère inviolé. Nous attendons toujours celui ou celle dont le nom vivra à jamais pour avoir su faire chanter les nombres premiers”.

BIBLIOGRAPHIE.

C. K. CALDWELL : "*La page des nombres premiers*", http://www.utm.edu/research/primes/.

A. DAHAN-DALMEDICO : "*Une histoire des mathématiques*", Poche, 1986.

P. DAMPHOUSSE : "*L'Arithmétique ou l'art de compter*", Broché, 2002.

J-P DELAHAYE : "*Merveilleux nombres premiers, voyage au coeur de l'arithmétique*", BELIN, Pour la science, 2000.

G. DUBERTRET : "*Initiation à la cryptographie*", Broché, 2002.

A. GRANVILLE : "*Nombres premiers et chaos quantiques*", Gazette des mathématiciens, Juillet 2003, SMF.

M. DE SAUTOY : "*La symphonie des nombres premiers*", éd. Héloïse d'Ormesson, 2004.

http://www-math.univ-fcomte.fr/pp_Annu/NJACON