Théorie des nombres

P. Rouchon

Ecole des Mines de Paris
Centre Automatique et Systèmes

Décembre 2007

Plan

Quelques références

- Excellent résumé dans le premier chapitre du cours ENST de Zémor.
- “Que sais-je” sur les nombres premiers (un éclairage probabiliste ainsi qu’une preuve élémentaire mais assez difficile du théorème des nombres premiers).
- Excellent livre de vulgarisation de Jean-Paul Delahaye sur les nombres premiers aux éditions Belin.
- l’Encyclopeadia Universalis comporte d’excellents articles sur des sujets connexes.
- Le livre classique dû à Hardy et Wright.
- Les carnets de Ramanujan

- On note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes modulo n. Il y en a n ($\#\mathbb{Z}_n = n$) et on identifie $\mathbb{Z}_n$ à l'ensemble $\{0, 1, ..., n-1\}$. $\mathbb{Z}_n$ est muni d'une structure naturelle d'anneau pour l'addition et la multiplication.
- Si $k \in \mathbb{Z}_n$ est inversible, on calcule son inverse via l'algorithme d'Euclide et l'identité de Bezout. On note $\mathbb{Z}_n^*$ l'ensemble des $k \in \mathbb{Z}_n$ inversibles.
- $\mathbb{Z}_n$ est un corps ssi n est premier et alors $\mathbb{Z}_n^* = \mathbb{Z}_n/\{0\}$ dans ce cas.

- Soient donc deux entiers strictement positifs $k < n$:

$$\begin{aligned} n &= kq_0 + r_0, \quad r_0 < k \\ k &= r_0 q_1 + r_1, \quad r_1 < r_0 \\ r_0 &= r_1 q_2 + r_2, \quad r_2 < r_1 \\ &\vdots \\ r_{m-2} &= r_{m-1} q_m + r_m, \quad r_m < r_{m-1} \\ r_{m-1} &= r_m q_{m+1} + r_{m+1}, \quad 0 = r_{m+1} < r_m \end{aligned}$$

où la suite $(n, k, r_0, r_1, ..., r_m, r_{m+1})$ est strictement décroissante et arrive à zéro avec $r_{m+1} = 0$.

- Le pgcd est r_m et on a u et v tels que

$$un + vk = \text{pgcd}\,(n, k) \quad \text{Identité de Bezout}$$

- Matrices uni-modulaires: matrices à coefficients entiers et dont l'inverse est aussi à coefficients entiers (système linéaire d'inconnue $(r_0, \ldots, r_m)$).

- Evaluons le nombre D de divisions de l'algorithme d'Euclide en fonction de la taille de n. L'algorithme est le plus long lorsque chaque quotient q_i vaut 1.
- $r_{m+2} = 0$, $r_m = r_{m-1} = 1$ et

  $$r_i = r_{i+1} + r_{i+2}, \quad i = 0, \ldots, m-2 \quad \text{avec} \quad k = r_0 + r_1, \quad n = k + r_0$$

- n correspond au $(m+4)$-ième nombre de la suite de Fibonacci où apparaît le nombre d'or $\phi = (1+\sqrt{5})/2$:

  $$F_j = F_{j-1} + F_{j-2}$$

  avec comme départ de la récurrence, $F_0 = 0$ et $F_1 = 1$.
- Comme $F_j = (\phi^j - (1-\phi)^j)/\sqrt{5}$ et $F_{m+4} = n$ on a au plus $D \leq \log_\phi(n)$ divisions avec reste à faire (Lamé (1845)).

- Pour tout entier $n > 1$, on note $\varphi(n)$ le nombre d'entiers entre 1 et $n-1$ premiers avec n:

$$\varphi(n) = \#\mathbb{Z}_n^*.$$

- Théorème de Fermat-Euler: Si a est premier avec n alors $a^{\varphi(n)} = 1 \mod (n)$ (preuve via $\prod_{x\in\mathbb{Z}_n^*} x = \prod_{x\in\mathbb{Z}_n^*} ax \mod (n)$).
- Lorsque n est premier $\varphi(n) = n-1$ on a le petit théorème de Fermat: si n est premier et si a entier entre 1 et $n-1$, alors $a^{n-1} = 1 \mod (n)$.

- Théorème d'Euler:

$$\sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d) = n$$

- Preuve: pour $1 \leq d \leq n$, on pose

$$\psi(d, n) = \#\{x \in \{0, \ldots, n-1\} \mid \text{pgcd}\,(x, n) = d\}.$$

Si d divise n alors $\psi(d, n) \neq 0$ sinon $\psi(d, n) = 0$. Donc $n = \sum_{d=1}^{n} \psi(d, n) = \sum_{d|n} \psi(d, n)$. Mais, $\psi(d, n) = \varphi(n/d)$ si d divise n. Il suffit de diviser par d, pour mettre en bijection les nombres x tels que pgcd $(x, n) = d$ et les nombres y tels que pgcd $(y, n/d) = 1$. Ainsi on a

$$n = \sum_{d|n} \varphi(n/d) = \sum_{d/n} \varphi(d).$$

- Théorème Chinois: soient deux entiers p et $q \geq 1$ et premiers entre eux. Alors les anneaux $\mathbb{Z}_p \times \mathbb{Z}_q$ et $\mathbb{Z}_{pq}$ sont isomorphes.
- Preuve: l'application $\pi : \mathbb{Z} \mapsto \mathbb{Z}_p \times \mathbb{Z}_q$ qui à $x \in \mathbb{Z}$ associe $(x \mod (p), x \mod (q))$ est un homomorphisme d'anneau, surjectif et de noyau $pq\mathbb{Z}$. Il suffit de quotienter par le noyau pour avoir un isomorphisme entre $\mathbb{Z}/pq\mathbb{Z} = \mathbb{Z}_{pq}$ et $\mathbb{Z}_p \times \mathbb{Z}_q$.
- Corollaire: si p et q sont premiers entre eux, alors $\varphi(pq) = \varphi(p)\varphi(q)$
- Corollaire: Si n admet comme décomposition en facteurs premiers $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$ alors

$$\varphi(n) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$$

- On part d'un grand nombre n (d'au moins 1024 bits) qui est le produit de deux grands nombres premiers p et q: clé publique n et e inversible modulo $\varphi(n) = (p-1)(q-1)$, clé secrète (p, q).
- Chiffrement d'un message en clair défini par un entier M mod (n) se fait par la transformation suivante:

$$M \mapsto M^e \mod (n).$$

- Déchiffrement: Bob reçoit via un canal public $A = M^e$. Pour déchiffrer, il lui suffit d'élever A à la puissance d où d est l'inverse de e modulo $\varphi(n) = (p-1)(q-1)$.

$$A^d = M \mod (n).$$

Pourquoi a-t-on $M^{ed} \equiv M \mod (n)$?

- La base du déchiffrement RSA via la clé secrète d du message chiffré M^e. :

$$\forall M \in \{0, 1, ..., n-1\}, \quad M^{ed} = M \mod (n)$$

dès que $n = pq$ où p et q sont deux nombres premiers, $e \in \{1, ..., \varphi(n-1)\}$ inversible modulo $\varphi(n)$ et d'inverse $d \in \{1, ..., \varphi(n-1)\}$

- Si M et n sont premiers entre eux, alors par le théorème d'Euler-Fermat $M^{\varphi(n)} = 1 \mod (n)$. Ainsi

$$M^{ed} = M^{1+k\varphi(n)} = M \mod (n).$$

- Si M et n non premiers entre eux, utiliser l'isomorphisme de la preuve du théorème chinois.

- Théorème de l'élément primitif: si p est premier alors, le groupe $(\mathbb{Z}_p^*, \times)$ est cyclique, i.e., il est de la forme

$$\mathbb{Z}_p^* = \{1, a, a^2, ..., a^{p-2}\}$$

où $a \in \mathbb{Z}_p^*$ est appelé élément primitif (non nécessairement unique).

- Preuve: le nombre d'éléments primitifs a est $\varphi(p-1)$ ($\sum_{d=1}^{p-1} N_d = p-1$ où N_d est le nombre d'éléments d'ordre d. N_d vaut soit 0 ou est supérieur à $\varphi(d)$. Conclure par théorème d'Euler en montrant, lorsque d divise $p-1$, que $N_d = \varphi(d)$.

- Théorème de Lucas: le nombre n est premier, si et seulement si, il existe $\alpha \in \mathbb{Z}_n^*$ tel que $\alpha^{n-1} = 1 \mod (n)$ et $\alpha^{\frac{n-1}{p}} \neq 1 \mod (n)$ pour tout diviseur premier p de $n-1$.
- Preuve: Si n est premier alors il suffit de prendre pour α un élément primitif modulo n. Inversement, si un tel élément α existe alors il est forcément d'ordre $n-1$ dans $\mathbb{Z}_n^*$. Or tout élément de $\mathbb{Z}_n^*$ est d'ordre un diviseur de $\varphi(n)$ (reprendre des bouts de la preuve du théorème sur l'élément primitif). Comme $\varphi(n) \leq n-1$ on voit que nécessairement $\varphi(n) = n-1$ mais cela signifie n premier.

Ce qu'on appelle la théorie analytique des nombres ne peut pas être considéré comme une théorie mathématique au sens usuel qu'on donne à ces mots, c'est-à-dire un système organisé de définitions et de théorèmes généraux accompagné d'applications à des exemples importants. Il s'agit au contraire ici presque exclusivement de problèmes particuliers qui se posent en arithmétique et qui, pour la plupart, consistent à étudier l'allure à l'infini de certaines fonctions définies par des conditions de nature arithmétique: par exemple le nombre $\pi(x)$ de nombres premiers $p \leq x$ ou le nombre $U(n)$ des solutions de l'équation $(x_1)^2 + (x_2)^2 = n$ en nombres entiers (x_1, x_2). Depuis 1830, on a imaginé, pour résoudre ces questions, des méthodes d'une extraordinaire ingéniosité qui consistent à associer aux fonctions arithmétiques étudiées des fonctions analytiques auxquelles on peut appliquer la théorie de Cauchy ou l'analyse harmonique; mais, malgré les succès spectaculaires obtenus par ces méthodes, on ne peut dire que l'on en comprenne vraiment les raisons profondes.

- La méthode consiste à associer à une suite d'entiers a_n (définis par une construction arithmétique (nombre de solutions d'une équation dépendant de n, cardinal d'un certain ensemble d'entiers plus petits que n, ...)) une série formelle.
- Le plus simple est de considérer la série

$$S(X) = \sum_{n \geq 0} a_n X^n$$

mais il faut être souvent plus malin comme nous le verrons avec les nombres premiers p_n.

- Suite à des manipulations astucieuses on propose une autre écriture de cette série que l'on manipule alors avec les règles usuelles de calcul sur les fonctions de la variable complexe (dérivée, résidu, intégrale de Cauchy, ...).
- Les informations sur les a_n, pour des grands indices n sont reliées aux singularités de la fonction analytique attachée à la série S.

- a_n est le nombre de solutions en entiers ≥ 0 de $x + 2y + 3z = n$.
- Alors

$$\sum_{n\geq 0} a_n X^n = \frac{1}{(1-X)(1-X^2)(1-X^3)}.$$

car

$$\frac{1}{1-X} = 1 + X + X^2 + X^3 + \ldots$$

- Maintenant pour calculer a_n, il vaut mieux passer par la décomposition en éléments simples ($j = \exp(2\imath\pi/3)$)

$$\frac{1}{(1-X)(1-X^2)(1-X^3)} = \frac{1}{6(1-X)^3} + \frac{1}{4(1-X)^2} + \frac{17}{72(1-X)} + \frac{1}{8(1+X)} + \frac{1}{9(1-jX)} + \frac{1}{9(1-j^2X)}.$$

- Comme $a_n = \frac{d^n S}{dX^n}(0)/(n!)$ on calcule cette dérivée n-ième sur la décomposition en éléments simples
- En utilisant l'identité

$$\frac{d^n}{dX^n}\left(\frac{1}{(1-\beta X)^\alpha}\right)_{X=0} = \beta^n \alpha(\alpha+1)...(\alpha+n-1)$$

on obtient

$$a_n = \frac{(n+1)(n+2)}{12} + \frac{n+1}{4} + \frac{17}{72} + \frac{(-1)^n}{8} + \frac{j^n + j^{2n}}{9}.$$

- Si nous nous intéressons à une estimation de a_n pour n grand, il suffit de considérer le pôle de degré le plus élevé $X = 1$, les autres donnant des contributions en n au plus. Ainsi, la structure des singularités de $S(X)$, i.e., de ces pôles, donnent les asymptotiques de a_n pour n grand.

- Ce phénomène est très général: Soient r entiers > 0, q_1, ..., q_r, sans diviseurs communs autre que 1. Notons a_n le nombre de solutions en entiers strictement positifs $(x_1, ..., x_r)$ de l'équation diophantienne

$$q_1 x_1 + ... + q_r x_r = n$$

- Alors $a_n \sim \frac{n^{r-1}}{q_1 ... q_r (r-1)!}$. Utiliser la série génératrice

$$\frac{1}{(1 - X^{q_1})...(1 - X^{q_r})}$$

et son pôle de plus haut degré $X = 1$.

Voici un autre exemple donné par Jacobi à l'aide de sa théorie des fonctions elliptiques. Le problème consiste à chercher le nombre de solutions a_n en nombres entiers (positifs ou négatifs) d'une équation à r inconnues:

$$x_1^2 + ... + x_r^2 = n$$

Ce nombre a_n est le coefficient de X^n dans la série de $(F(X))^r$ où

$$F(X) = \sum_{m \in \mathbb{Z}} X^{m^2}.$$

Cette série converge pour $X \in \mathbb{C}$ de module plus petit que 1.

- Le nombre de partitions $p(n)$ d'un entier $n \geq 0$ est par définition le nombre de solutions en entiers $x_i > 0$ de

$$x_1 + 2x_2 + \ldots + mx_m + \ldots = n$$

où le nombre d'inconnues m n'est pas limité

- La série génératrice, convergente pour $|X| < 1$, est donnée par:

$$S(X) = \sum_{n=0}^{\infty} p(n)X^n = \prod_{m=1}^{\infty} (1 - X^m)^{-1}.$$

- $p(n)$ à l'aide de la formule de Cauchy $p(n) = \frac{1}{2\imath\pi} \oint_{\mathcal{C}} \frac{S(z)}{z^{n+1}} dz$ où $\mathcal{C}$ est un lacet entourant 0 à l'intérieur du disque unité.
- En évaluant cette intégrale selon un contour $\mathcal{C}$ bien choisi et tendant vers le cercle unité, Hardy et Ramanujan ont montré que $p(n) \sim \frac{1}{4\sqrt{3n}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$.

- On note $(p_n)_{n\geq 1}$ les nombres premiers rangés par ordre croissant: Euler a "codé" la suite des p_n dans une fonction de la variable complexe s

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}.$$

- Le lien entre ζ et les nombres premiers vient du calcul génial suivant du à Euler:

$$\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}} = \prod_{p\in\mathbb{P}} (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ldots).$$

En développant ce produit infini, nous voyons qu'il fait intervenir $\frac{1}{p_1^{\alpha_1 s}} \ldots \frac{1}{p_k^{\alpha_k s}}$ pour k entier et α_i entier et p_i premier.

- C'est maintenant en jouant sur les deux formes de ζ, la série de Dirichlet $\sum 1/n^s$ et le produit eulérien $\prod 1/(1-1/p^s)$ que l'on obtient des informations sur les grands nombres premiers.

- Dès 1737, Euler avait utilisé ζ comme fonction de la variable réelle s pour étudier la suite p_n.
- L'équivalent $\pi(x) \sim x/\log(x)$, le nombre de p_n plus petits que l'entier x, avait été conjecturé par Gauss et Legendre à la fin du XVIIIème siécle.
- Il a fallut cependant attendre le milieu du XIXème siècle pour que Tschebyschef établisse par des moyens arithmétiques élémentaires qu'il existe deux constantes A et B, $0 < A < 1 < B$ telles que, pour x assez grand

$$A\frac{x}{\log(x)} < \pi(x) < B\frac{x}{\log(x)}.$$

- Ce n'est qu'en 1896 que Hadamard et de la Vallée-Poussin démontrèrent indépendamment le théorème sur des nombres premiers, i.e., le fait que $\pi(x) \sim x/\log(x)$ lorsque $x \mapsto +\infty$.
- Pour cela, ils se sont fortement appuyés sur le célèbre article de Riemann en 1859 qui montrait que ζ admettait un prolongement méromorphe pour $s \in \mathbb{C}$ et aussi qui mettait en évidence de façon largement conjecturale le lien entre la distribution des zéros de ζ et celle des nombres premiers.
- La relation entre la fonction ζ et la fonction entière ξ qui vérifie $\xi(s) \equiv \xi(1-s)$ $\left(\Pi(s) = \Gamma(s+1) = \int_0^{+\infty} e^{-x} x^s dx\right)$:

$$\xi(0) \prod_1^{\infty} \left(1 - \frac{s}{\rho_n}\right) = \xi(s) = \Pi(s/2)(s-1)\pi^{-s/2}\zeta(s).$$

ξ code les zéros non triviaux ρ_n de ζ. On pense (hypothèse de Riemann) que $\Re(\rho_n) = 1/2$, pour tout n.

- Pour $\Re(s) > -1$ l'intégrale $\int_0^{+\infty} e^{-x} x^s dx$ est absolument convergente et définit la fonction $\Pi(s)$ ($\Gamma(s) = \Pi(s-1)$) sur le demi-plan complexe $\Re(s) > -1$ avec pour $n \in \mathbb{N}$: $\Pi(n) = n!$.
- Une simple intégration par partie montre que $\Pi(s+1) = (s+1)\Pi(s)$ pour $\Re(s) > -1$. On prolonge alors sans ambiguïté $\Pi(s)$ pour tout $s \in \mathbb{C}$ sauf en $s = -n$, $n \in \mathbb{N}$, $n \geq 1$ où Π admet des pôles de multiplicité 1: $\Pi(s) = \frac{\Pi(s+n)}{(s+1)...(s+n)}$.

Ainsi la fonction $\Pi(s)$ est définie sur $\mathbb{C}$ sauf pour les entiers strictement négatifs où elle admet des pôles simples. Dans son fameux article de 1859, Riemann propose un prolongement similaire en partant de $\sum_{n>1} n^{-s}$ au lieu de $\int_0^{+\infty} e^{-x} x^s dx$, mais cette fois le prolongement est possible pour $s \in \mathbb{C}$ avec $s \neq 1$ où on a un pôle simple.

- La série $\sum_{n\geq 1} n^{-s}$ est absolument convergente pour tout complexe s dès que $\Re(s) > 1$. Elle définit la fonction $\zeta(s)$ sur le demi-plan $\Re(s) > 1$.
- Avec $\int_0^{+\infty} e^{-nx} x^{s-1} dx = \frac{\Pi(s-1)}{n^s}$ on montre que, pour $\Re(s) > 1$:

$$\Pi(s-1)\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right) = \int_0^{+\infty} \frac{x^{s-1}}{e^x - 1} dx$$

- Avec la détermination standard du log sur $\mathbb{C}/\mathbb{R}^-$: $\log z = \log r + i\theta$ pour $z = re^{i\theta}$ avec $r > 0$ et $\theta \in]-\pi, \pi[$ on a, via le théorème de Cauchy,

$$\int_\gamma \frac{(-z)^s}{e^z - 1} \frac{dz}{z} = 2i \sin(\pi s) \int_0^{+\infty} \frac{x^{s-1}}{e^x - 1} dx$$

où γ est le contour suivant parcouru dans le sens direct: $z = t + i$ pour t réel de $+\infty$ à 0; ensuite $z = e^{it}$ pour t réel allant de $\pi/2$ à $3\pi/2$; enfin $z = t - i$ pour t réel de 0 à $+\infty$.

Pour $\Re(s) > 1$:

$$\int_\gamma \frac{(-z)^s}{e^z - 1} \frac{dz}{z} = 2i \sin(\pi s)\Pi(s-1)\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)$$

Avec l'identité $\sin(\pi s) = \frac{\pi s}{\Pi(s)\Pi(-s)}$ on a

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{\Pi(-s)}{2i\pi} \int_\gamma \frac{(-z)^s}{e^z - 1} \frac{dz}{z}.$$

Compte tenu de la forme du contour γ (entoure $\mathbb{R}^+$), la fonction $s \mapsto \int_\gamma \frac{(-z)^s}{e^z-1} \frac{dz}{z}$ est définie pour tout $s \in \mathbb{C}$: c'est une fonction entière de s. On peut ainsi utiliser la formule précédente pour prolonger $\zeta(s)$ lorsque $\Re(s) \leq 1$ et $s \neq 1$. Autour de $s = 1$, $\zeta(s)$ explose comme Π en -1 (pôle simple).

- Théorème des nombres premiers: On note $\pi(x)$, le nombre des entiers premiers et plus petits que $x > 0$. Alors, lorsque x tend vers $+\infty$, $\pi(x) \sim x/\log(x)$. Ceci est équivalent à dire que $p_n \sim n\log(n)$ lorsque n tend vers $+\infty$.
- Nous allons donner une "preuve" heuristique et suggestive en utilisant la fonction $\zeta(s)$ comme produit eulérien

$$\sum_{n\geq 1} 1/n^s = \zeta(s) = \prod_{n\geq 1}(1 - 1/p_n^s)^{-1}$$

pour $s > 1$ réel tendant vers 1.

- L'idée essentielle est de prendre le log:

$$\log(\zeta(s)) = -\sum_{n\geq 1} \log(1 - 1/p_n^s)$$

- comme $\forall y \in [0, 1/2], \quad y \leq -\log(1-y) \leq y + y^2/2$ on a

$$\sum_{n\geq 1} \frac{1}{p_n^s} \leq \log(\zeta(s)) \leq \sum_{n\geq 1} \frac{1}{p_n^s} + \sum_{n\geq 1} \frac{1}{2p_n^{2s}}.$$

- Comme $\lim_{s\mapsto 1^+} \zeta(s) = +\infty$ la série, $\sum 1/p_n$ est aussi divergente. Donc il n'existe pas de constantes A et $\epsilon > 0$ telles que $p_n \geq An^{1+\epsilon}$ pour tout n.

- Comme chacun des termes du produit est plus grand que 1, on a
$$\zeta(s) \geq \prod_{p_n \leq N} (1 - 1/p_n^s)^{-1}.$$
Avec $(1 - 1/p_n^s)^{-1} = \sum_{k \geq 0} 1/p_n^{ks}$ on voit que
$$\prod_{p_n \leq N} (1 - 1/p_n^s)^{-1} = \sum_{n \in E_N} 1/n^s$$
où E_N est l'ensemble des entiers dont les diviseurs premiers valent au plus N. Il est clair que E_N contient au moins $\{1, ..., N\}$.
- Cela suggère que $\sum_{1 \leq n \leq N} 1/n$ et $\prod_{p_n \leq N}(1 - 1/p_n)^{-1}$ sont similaires pour N grand.
- Comme
$$\log\left(\sum_{1 \leq n \leq N} 1/n\right) = \log(\log(N)) + O(1)$$

- Si n est premier alors $\pi(n) - \pi(n-1) = 1$, sinon $\pi(n) - \pi(n-1) = 0$. Donc

$$\sum_{p_n \leq N} 1/p_n = \sum_{1 \leq n \leq N} (\pi(n+1) - \pi(n))/n$$

- En réorganisant cette somme et comme $\pi(N+1) \leq N$, on voit que

$$\sum_{p_n \leq N} 1/p_n = \sum_{1 \leq n \leq N-1} \pi(n)/(n(n+1)) + O(1).$$

Mais aussi on a

$$\log(\log(N)) = \sum_{1 \leq n \leq N-1} 1/(n\log(n)) + O(1).$$

- Ainsi il est tentant de conjecturer que

$$\pi(n)/(n(n+1)) \sim 1/(n\log(n)$$

soit $\pi(n) \sim n/\log(n)$.

- Progression arithmétique: Soient a et m des entiers strictement positifs et premiers entre eux. Il existe une infinité de nombres premiers de la forme $a + km$ avec k entier positif.
- En fait ce théorème admet une formulation nettement plus précise: les nombres premiers se distribuent uniformément parmi les $\varphi(m)$ classes associées aux nombres a plus petits que m et premiers avec lui.
- Si on note $\pi_a(x)$ le nombre d'entiers premiers plus petits que x et de la forme $a + km$, alors on a l'asymptotique suivante pour $x \mapsto +\infty$:

$$\pi_a(x) \sim \frac{1}{\varphi(m)}\pi(x) = \frac{x}{\varphi(m)\log(x)}.$$

La philosophie générale sous-jacente à de nombreuses conjectures sur les nombres premiers: tout ce qui n'est pas trivialement interdit est en fait réalisé:

- nombres premiers jumeaux: il existe une infinité de nombres premiers p tels que $p+2$ soit aussi premier.
- nombres premiers cousins: il existe une infinité de nombres premiers p tels que $p+4$ et $p+6$ soient aussi premiers.
- C. Goldbach, un contemporain d'Euler, avait émis en 1742 la conjecture que tout entier pair est somme de deux nombres premiers et tout entier impair somme de trois nombres premiers.

- Preuve du théorème de la progression arithmétique pour $m = 4$. Deux valeurs possibles pour a: 1 ou 3.
- Soient les deux fonctions χ_0 et χ_2 de $\mathbb{N}$ vers $\{-1, 0, 1\}$ définies par

$$\chi_0(n) = \begin{cases} 1 \text{ si } n = 1 \text{ou} 3 \bmod(4) \\ 0 \text{ sinon} \end{cases} \qquad \chi_1(n) = \begin{cases} 1 \text{ si } n = 1 \bmod(4) \\ -1 \text{ si } n = 3 \bmod(4) \\ 0 \text{ sinon} \end{cases}$$

  χ_0 et χ_1 sont périodiques (période 4) et multiplicatives, i.e., $\chi_0(nm) = \chi_0(n)\chi_0(m)$ et $\chi_1(nm) = \chi_1(n)\chi_1(m)$ pour tout couple d'entiers (n, m).
- Cette propriété est essentielle pour associer à chacune de ces fonctions multiplicatives une série de Dirichlet qui s'exprime sous la forme d'un produit eulérien.

- On pose $\zeta_0(s) = \sum_{n\geq 1} \frac{\chi_0(n)}{n^s}$, $\zeta_1(s) = \sum_{n\geq 1} \frac{\chi_1(n)}{n^s}$, . Considérons maintenant les produits suivants: $\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{\chi_0(p)}{p^s}}$ et $\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{\chi_1(p)}{p^s}}$.
- Comme χ_0 et χ_1 sont multiplicatives, on voit en développant ces produits que

$$\zeta_0(s) = \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{\chi_0(p)}{p^s}}, \quad \zeta_1(s) = \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{\chi_1(p)}{p^s}}.$$

- Avec $-\log(1-y) = y + w(y)y^2$ pour $|y| \leq 1/2$ avec w régulière:

$$\log(\zeta_0) = \sum_{p\in\mathbb{P}} \frac{\chi_0(p)}{p^s} + h_0(s), \quad \log(\zeta_1) = \sum_{p\in\mathbb{P}} \frac{\chi_1(p)}{p^s} + h_1(s)$$

où h_0 et h_1 sont des fonctions régulières de s et définies en $s = 1$.

- On a
$$\zeta_0(s) = \sum_{k\geq 0}\left(\frac{1}{(4k+1)^s} + \frac{1}{(4k+3)^s}\right).$$
Ainsi, lorsque s est réel et tend vers 1 par valeur supérieure, $\zeta_0(s)$ tend vers $+\infty$.
- Par contre ζ_1 reste borné autour de $s = 1$ car
$$\zeta_1(s) = \sum_{k\geq 0}\left(\frac{1}{(4k+1)^s} - \frac{1}{(4k+3)^s}\right)$$
où $\frac{1}{(4k+1)^s} - \frac{1}{(4k+3)^s}$ est équivalent lorsque k tend vers l'infini à $\frac{s}{2^{2s+1}k^{s+1}}$. De plus chaque terme est strictement positif, donc $\zeta_1(1) = \sum_{k\geq 0}\frac{2}{(4k+1)(4k+3)} > 0$.

- Notons maintenant

$$P_1(s) = \sum_{\substack{p \in \mathbb{P} \\ p = 1 \bmod(4)}} \frac{1}{p^s}, \qquad P_3(s) = \sum_{\substack{p \in \mathbb{P} \\ p = 3 \bmod(4)}} \frac{1}{p^s}.$$

- Ainsi

$$\log(\zeta_0(s)) = P_1(s) + P_3(s) + h_0(s)$$
$$\log(\zeta_1(s)) = P_1(s) - P_3(s) + h_1(s)$$

- Comme, $\zeta_1(s)$, h_0 et h_1 sont régulières en $s = 1$, $\zeta_1(1) > 0$ et $\lim_{s \mapsto 1^+} \zeta_0(s) = +\infty$ on en déduit nécessairement que $\lim_{s \mapsto 1^+} P_1(s) = +\infty$ et $\lim_{s \mapsto 1^+} P_3(s) = +\infty$.

- La méthode que nous avons utilisée est en fait général. Donnons en une brève esquisse.
- Pour un entier $m > 2$ on a en fait $\varphi(m)$ choix possibles pour a, soit $a \in \mathbb{Z}_m^*$. Sur le groupe multiplicatif $\mathbb{Z}_m^*$ on définit l'analogue des fonctions χ_0 et χ_1, en fait $\varphi(m)$ fonctions $\chi_0, ..., \chi_{\varphi(m)-1}$ fonctions multiplicatives distinctes mais à valeurs dans le cercle unité: ce sont les caractères de Dirichlet. On note toujours le caractère trivial égal à 1 sur $\mathbb{Z}_m^*$ par χ_0. Les autres caractères χ_k, $k = 1, ..., \varphi(m) - 1$ se distinguent de χ_0 par le fait que

$$\sum_{a \in \mathbb{Z}_n^*} \chi_k(a) = 0.$$

- Pour $k \neq 0$, les séries de Dirichlet

$$\zeta_k(t) = \sum_{n \geq 1} \frac{\chi_k(n)}{n^s}$$

sont très différentes autour de $s = 1$ de la série ζ_0 associée à χ_0.

- Contrairement à ζ_0 qui diverge en $s = 1$, ces séries ζ_k sont des "séries alternées" (utiliser le critère d'Abel) et ainsi convergent en $s = 1$.
- Maintenant, chaque ζ_j s'exprime comme un produit eulérien.

$$\log(\zeta_j) = \sum_{p \in \mathbb{P}} \frac{\chi_j(p)}{p^s} + h_j(s),$$

où h_j est une fonction régulière de s définie autour de $s = 1$.

- On pose, pour $a \in \mathbb{Z}_m^*$,

$$P_a(s) = \sum_{\substack{p \in \mathbb{P} \\ p = a \bmod(m)}} \frac{1}{p^s}.$$

Alors on a

$$\log(\zeta_j(s)) = h_j(s) + \sum_{a \in \mathbb{Z}_n^*} \chi_j(a) P_a(s).$$

- Des calculs simples sur les caractères montrent que la matrice $\varphi(m) \times \varphi(m)$ d'éléments $\left(\chi_j(a)\right)$ pour $0 \leq j \leq \varphi(m) - 1$ et $a \in \mathbb{Z}_m^*$ est inversible, d'inverse sa conjuguée (hermitienne) divisée par $\varphi(m)$.
- Les $P_a(s)$ s'expriment comme des combinaisons linéaires à coefficients non nuls des $\log(\zeta_j)$ et des h_j.

- La partie dure de la preuve est de montrer qu'aucune des valeurs prises en $s = 1$ par les ζ_k ($k \in \{1, ..., \varphi(m) - 1\}$) n'est nulle: $\zeta_k(1) \neq 0$.
- Comme $\zeta_0(s)$ est la seule à diverger en $s = 1$, on en déduit alors que chacun des $P_a(s)$ diverge en $s = 1$. Et donc $\{p \in \mathbb{P} \mid p = a \mod (m)\}$ est infini pour tout $a \in \mathbb{Z}_m^*$.
- On comprend un peu mieux pourquoi la localisation des zéros des fonctions de Dirichlet ζ_j est si importante. La conjecture de Riemann généralisée affirme que les zéros (à partie réelle positive) des ζ_j se situent tous sur la droite parallèle à l'axe imaginaire $\Re(s) = 1/2$.