Titre III
Les Outils de l'Horloger

III.1 Quelques outils courants

III.1.1 Infinitude et raréfaction des nombres premiers.

La quantité $\pi(x)$ des nombres premiers inférieurs ou égaux à x est asymptotique aux trois expressions de même origine mais de précision décroissante ci-dessous :

- D'après **Riemann :** $\lim_{x\to\infty}\pi(x) = R(x) = \sum_{n=1}^{\infty}\frac{\mu(n)}{n}\mathrm{li}\left(x^{1/n}\right)$, $\mu(n)$ étant ka fonction de **Moebius**
- $\lim_{x\to\infty}\pi(x) =$ Logarithme intégral $\mathrm{li}(x) = \int_2^x \frac{dt}{\ln(t)}$
- Selon **Hadamard** et **La Vallée Poussin)** : $\lim_{x\to\infty}\pi(x) = \frac{x}{\ln(x)}$

Les deux premières approximations sont difficilement maniables. La troisième est à utiliser avec précaution même pour des nombres importants: on sait que $\frac{x}{\ln(x)}$ donne toujours des valeurs notablement inférieures à la valeur réelle de $\pi(x)$. De plus, la quantité des nombres premiers inférieurs ou égaux à p_k n'est autre que k, si bien qu'une utilisation abusive conduit à

$$k = \frac{p_k}{\ln p_k}, \text{ d'où } \frac{k}{p_k}\ln p_k = 1$$

La limite atteinte dans le tableau prem-tableau-premiers.xlsb nous donne pour le nombre premier $p_k = 9\,998\,603$ d'où :

$\pi(p_k) = k = 664\,600$ au lieu de $\frac{p_k}{\ln p_k} = 620\,339$ qui représente une minoration absolue de $43\,661$ et une minoration relative de 7%.

Pire encore, l'utilisation de cette limite comme approximation pour les nombres pairs n courants conduirait à la négation de la conjecture de Goldbach ainsi qu'il sera démontré au titre VI.

III.1.2 Ecarts entre nombres premiers

De la dernière approximation de $\pi(x)$, il résulte que l'écart d_k entre le nombre premier p_k et le suivant p_{k+1} est tel que $\lim_{k\to\infty}\frac{d_k}{p_k}=0$.

Plus précisément **Hoheisel** a établi une relation montrant implicitement l'accroissement maximal des écarts en fonction de l'exposant $\theta = 7/13+e \quad \forall e>0$:

$$\pi\left(x+x^{\theta}\right)-\pi(x)\approx\frac{x^{\theta}}{\ln x}$$

III.1.3 Sommation des inverses des nombres premiers

La somme des inverses des nombres premiers croît très lentement :

$$\sum_{p\le n}\frac{1}{p}=\ln\ln n+M+o(1) \quad | \quad M=0.2615....\text{(Constante de }\textbf{Mertens}\text{)},$$

d'où : $\sum_{p\le n}\frac{1}{p}\simeq\ln\ln n$ lorsque n tend vers l'infini. (3.1)

Assimilant cette sommation à une intégrale, la dérivée en est $\frac{1}{n\ln n}=\frac{1}{\ln n^n}$ dont la valeur est de plus en plus faible avec n, dénotant une croissance de (3.1) vers l'infini qui ne cesse de ralentir.

III.1.4 Théorème de la progression arithmétique dû à Dirichlet

Parmi les nombres de la progression arithmétique $a \bmod b$, il existe une quantité illimitée de nombres premiers à condition que a et b soient premiers entre eux ; dans le cas contraire, cette progression ne comporte, au plus, qu'un seul nombre premier.

III.1.4.1 Extension du théorème de Dirichlet

Soit une progression arithmétique $aq+b$, où a et b sont premiers entre eux ; on démontre que la quantité ainsi produite de nombres premiers inférieurs à un nombre donné n, quantité que l'on baptise $\pi_{a,b}(n)$, tend vers $\frac{n}{\varphi(a)\ln n}$ lorsque n augmente indéfiniment, $\varphi(a)$ étant la fonction indicatrice d'Euler. Rappelons que cette fonction $\varphi(a)$ a pour valeur la quantité de nombres inférieurs à a et n'ayant aucun facteur premier avec a.

III.2 Des outils moins bien utilisés

III.2.1 Le théorème de Bachet de Méziriac

Faussement attribué à **Etienne Bézout**, le théorème de **Bachet** de **Méziriac** nous apprend que si deux nombres a et b ont un PGCD égal à c, alors il existe deux autres entiers x et y tels que l'on ait

$$xa + yb = c \tag{3.1}$$

Ce théorème se démontre en utilisant l'algorithme d'Euclide, lequel algorithme permet le calcul des coefficients x et y. Dans le cas où $c = 1$, la relation précédente devient caractéristique de la primalité relative de a et b**.**

Dans la relation de **Bachet** de **Méziriac**, les coefficients x, y ne sont pas uniques, car on trouve une quantité illimitée d'autres jeux (x', y'), lesquels sont liés à (x, y) par les relations

$$x' = x + kb$$
$$y' = y - ka$$

Mais, c'est le jeu (x, y) issu de l'algorithme d'Euclide qui, généralement, est implicitement retenu.

Le théorème de **Bézout**, tel que partout exprimé est donc incomplet et trompeur.

III.2.2 Le théorème des restes chinois

La plus large extension de ce théorème est la suivante :

Soient $n_1, ..., n_k$ des entiers premiers entre eux ; autrement dit : $\text{pgcd}(n_i, ..., n_k) = 1$

Si entre un entier x et une suite quelconque d'entiers $a_1, ..., a_k$, il existe un système de congruences

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ &..... \\ x &\equiv a_k \bmod n_k \end{aligned} \tag{3.2}$$

alors il existe une solution modulaire unique de ce système, laquelle s'écrit

$$x \equiv a \bmod \prod_{i=1}^{k} n_i$$

Cette solution peut être obtenue ainsi :

Posons $n = \prod_{i=1}^{k} n_i$, puis $m_i = \dfrac{n}{n_i}$; m_i et n_i sont premiers entre eux et satisfont donc la relation de **Bachet de Méziriac** d'après laquelle on peut trouver deux entiers u_i et v_i non nuls tels que

$$u_i n_i + v_i m_i = 1 \tag{3.3}$$

Posant $e_i = v_i m_i$, la relation ci-dessus entraîne

$$u_i n_i + e_i = 1 \ ;$$

On peut donc écrire $e_i \equiv 1 \bmod n_i$ et, comme $e_i = v_i m_i = v_i \dfrac{n}{n_i}$ est divisible par tout $n_{j\le k} \neq n_i$,

$$e_i = 0 \bmod n_{j\le k} \quad \text{si} \quad j \neq i$$

D'où la relation générale :

$$\begin{aligned} e_i &\equiv 1 \bmod n_i \\ e_j &\equiv 0 \bmod n_i \end{aligned} \quad \text{pour tout } j \neq i \qquad (3.4)$$

Dans ces conditions :

$$x = \sum_{i=1}^{k} a_i e_i \equiv a_i \bmod n_i \text{ , pour chaque } i = 1,...,k \text{ .}$$

Quelles sont les solutions pour les autres entiers $n_1,....,n_k$ différents de n_i ?

Si l'un d'eux est y, $\quad y - x \equiv 0 \bmod n_i \quad \forall n_i$

et par conséquent, $\quad y - x \equiv 0 \bmod \left(n = \prod_{i=1}^{k} n_i \right)$ car $n = \prod_{i=1}^{k} n_i$ est un multiple de n_i

Le système (3.2) admet donc une seule solution modulo $\boldsymbol{n}$, soit :

$$y \equiv x \bmod n \equiv \left(\sum_{i=1}^{k} a_i e_i \right) \bmod n$$

Le nombre de congruences d'un système peut-il être illimité ?

Oui, car à la solution d'un système de congruences tel que $x \equiv a \bmod n$, où $n = \prod_{i=1}^{k} n_i$, on peut toujours ajouter la solution d'un autre système de congruences, en appliquant 'en cascade' le théorème des restes.

III.3 Evaluation de la quantité de nombres premiers affectés de diverses conditions.

III.3.1 Exemples de conditions

Outre celle des nombres premiers, elles concernent, par exemple :

- les jumeaux premiers :

  leur paramètre commun q dans l'écriture $2q \pm 1$ est soumis à deux conditions sur les restes $r_{i\eta}$:

  $$q \equiv r_{i\eta} \bmod p_i \quad | \quad r_{i\eta} \neq \pm i\eta \quad | \quad \forall p_i = (2i + \eta) \le \left[\sqrt{2q+1} \right]$$

- les couples de nombres premiers dont la différence est égale à un nombre pair donné $2n$ (conjecture de **Polignac**) ; parmi eux les nombres cousins et sexy.

  $(2u+1) - (2v+1) = 2n$ peut aussi s'écrire $2v+1 = 2(u-n)+1$; donc $2u+1$ et $2v+1$ seront tous deux premiers si, et seulement si,

$$\begin{cases} u = r_i \bmod (2i+1) \\ u - n = r_i \bmod (2i+1) \end{cases} \rightarrow \quad u = n + r_i \bmod (2i+1)$$

Avec $\begin{cases} r_i \neq i \\ n + r_i \neq i \end{cases} \rightarrow \quad r_i \neq i - n \qquad \forall\,(2i+1)_{\text{premier}} \leq \left\lfloor \sqrt{2u+1} \right\rfloor$

Cette relation impose 2 conditions sur les restes r_i de la division de la suite des entiers u par la suite des nombres premiers successifs.

- les constellations

  Elles doivent respecter certaines formes plus faciles à écrire avec $p = 6q + \eta$: par exemple, la suite

  $p, p+2, p+10$ est impossible parce que $p+2$ impose $p = 6q-1,\ p+2 = 6q+1$ et par conséquent $p+10 = 6q-1+10 = 6q-9$ qui est divisible par 3**.**

  Par contre, est possible la suite

  $$6q+1, \quad 6q+1+4 = 6(q+1)-1, \quad 6q+1+6 = 6(q+1)+1,$$
  $$6q+1+10 = 6(q+2)-1, \quad 6q+1+12 = 6(q+2)+1$$

  Ses termes seront tous premiers si, et seulement si, les 5 conditions suivantes sont respectées sur les restes du paramètre le plus élevé, c'est-à-dire $(q+2)$:

  $$\left[r_i \neq i\eta - 2, \quad r_i \neq -i\eta + 1, \quad r_i \neq i\eta - 1, \quad r_i \neq -i\eta, \quad r_i \neq i\eta \right]$$
  $$\forall\,(6i+\eta)_{\text{premier}} \leq \left\lfloor \sqrt{6(q+2)+1} \right\rfloor$$

  Suivant les premiers $6i+\eta$, certaines conditions peuvent être redondantes, ainsi :
  pour $6i-1=5$, les restes interdits sont $-3, 0, -2, 1, -1$
  tandis que pour $6i+1=7$, ils deviennent $-1, 0, 0, -1, +1$

  Dans le deuxième cas, il ne reste que 3 conditions au lieu de 5**.**

  Ces conditions s'appliquent à la division de tous les entiers q successifs par la suite des nombres premiers.

III.3.2 Démonstration de l'infinitude des nombres premiers liés par plusieurs conditions

Soit cr le nombre de conditions sur chacun des restes r_j de la division de $2q+1$ par les nombres premiers successifs p_j . Les paramètres q des nombres premiers par rapport à la séquence des nombres strictement premiers $p_1, \ldots, p_k$ s'écrivent :

$$q \equiv r_j \bmod p_j \quad | \quad r_j \neq 0 \quad \forall\,(1 < p_j \leq p_k)$$

Mais selon les cas, il doit exister $p_j - cr$ valeurs admissibles des restes r_j , ce qui fait que seuls les premiers p_j supérieurs à cr peuvent être pris en compte.
On doit donc utiliser une écriture plus élaborée des nombres premiers étudiés. Si p_a est le nombre premier immédiatement inférieur à cr, on devra recourir à une expression première par rapport à tous les nombres premiers inférieurs ou égaux à p_a , et par conséquent utiliser une écriture de base $\prod_{i=1}^{a} p_i$, soit :

$$2w+1 = q \times \prod_{i=1}^{a} p_i \pm r \text{ avec } r \text{ non divisible par } (2,3,...,p_a)$$

Les différents paramètres q_n admissibles sont alors chacun définis par des systèmes de congruences dont les solutions relèvent du théorème des restes chinois, soit

$$q_n \equiv r_{a+1} \bmod p_{a+1}$$
$$.....$$
$$q_n \equiv r_k \bmod p_k$$

Posant $\prod_{j=a+1}^{j=k} p_j = \Pi_k$, on trouve d'après **Bachet de Méziriac** deux entiers u_j et v_j tels que

$$u_j p_j + v_j \Pi_k / p_j = 1.$$

Posant $e_j = v_j \Pi_k / p_j$, à la $n^{ème}$ collection des restes r_j correspond une unique solution

$$q_{nk} \equiv \left(\sum_{j=a+1}^{k} r_j e_j \right) \bmod \Pi_k$$

On remarque que $\sum_{j=a+1}^{k} r_j e_j$ est le produit scalaire de deux vecteurs (r_j) et (e_j) dont la dimension est $k-a$.

Posant $(r_j) = \overrightarrow{r_{nk}}$ et $(e_j) = \overrightarrow{e_k}$ on écrit : $q_{nk} \equiv \overrightarrow{r_{nk}} \cdot \overrightarrow{e_k} \bmod \Pi_k$ (3.5)

L'indice n repère la collection des composantes r_j du vecteur $\overrightarrow{r_{nk}}$ retenu.

L'indice n repère aussi la solution q_{nk} correspondante attribuée au paramètre q_n retenu.

L'indice k indique les nombres premiers de la séquence $p_{a+1},...,p_k$.

Dès que le plus grand nombre premier p_k est fixé, chaque composante du vecteur $\overrightarrow{e_k}$ a une valeur déterminée. Par contre, chaque composante des vecteurs $\overrightarrow{r_{nk}}$ associée aux facteurs premiers p_j peut avoir une des $p_j - cr$ valeurs permises.

Le premier intervalle $(0 - \Pi_k)$ de l'analyse modulaire comporte

- les paramètres éliminés des nombres composés de facteurs $p_j \quad | \quad p_{a+1} \le p_j \le p_k$,
- les paramètres q_{nk} conservés de nombres composés de facteurs supérieurs à p_k ,
- des paramètres q_{nk} des nombres strictement premiers (dont tous ceux qui sont inférieurs à p_{k+1}^2 s'ils existent).

Les vecteurs $\overrightarrow{r_{nk}}$ ont $k - cr$ dimensions ; la $(k-cr)_{ème}$ dimension possède une quantité de composantes admissibles égale à $p_k - cr$, multipliant ainsi par $p_k - cr$ la quantité de composantes des vecteurs précédents. La quantité de composantes des vecteurs $\overrightarrow{r_{nk}}$ et par conséquent celle des solutions q_{nk} est donc :

$$N_k = (p_{a+1} - cr) \times (p_{a+2} - cr) \times .... \times (p_k - cr) \quad (3.6)$$

III.3.3 Infinitude des nombres premiers liés par *cr* conditions

La quantité $N_k = (p_{a+1} - cr)....(p_k - cr)$ augmente sans cesse avec p_k.

Les nombres premiers jusqu'en p_k ainsi trouvés appartiennent à une série d'intervalles

$$\prod_{j=a+1}^{k} p_j, \ldots, x\prod_{j=a+1}^{k} p_j, (x+1)\prod_{i=a+1}^{k} p_j, \ldots$$

dont la taille est considérablement supérieure à p_k .

Cependant, lorsque p_k devient infini, N_k **devient une quantité infinie de nombres strictement premiers.**

Devant cet aspect choquant pour notre vision immédiate, nous sommes obligés de recourir au concept de l'infini selon **Cantor**.

Cantonnons-nous au premier intervalle qui nous fournit les résultats significatifs à $x\prod_{j=a+1}^{k} p_j$ près.

La suite illimitée des quantités N_k pour cr conditions appartient à un ensemble dénombrable que nous baptisons E_{cr} .

Chaque élément N_k est lié par son indice au nombre premier p_k et par conséquent à l'entier naturel k, et inversement**,** ce qui crée une relation biunivoque entre les éléments de E_{cr} et les nombres entiers $k > a$. Les entiers $(1, \ldots, a)$ composent un ensemble dénombrable fini. Donc E_{cr} privé de $(1, \ldots, a)$ reste équipotent avec l'ensemble des entiers naturels.

D'où l'importante propriété :

> Les sous-ensembles de nombres premiers jusqu'en p_k et qui sont liés par une quantité finie de conditions sont en une même quantité infinie $\aleph_0$ que les nombres entiers.
>
> Lorsque p_k tend vers l'infini, ces sous-ensembles tendent vers des sous-ensembles de nombres strictement premiers.

III.3.4 Densité limite des nombres premiers liés par *cr* conditions

La densité de tels nombres est : $$\frac{(p_{a+1} - cr)....(p_{k+1} - cr)}{\prod_{i=a+1}^{k} p_i} < \prod_{i=a+1}^{k} (1 - cr/p_i)$$

Rapporté à celle des nombres premiers sur les mêmes intervalles, cela donne :

$$\prod_{i=a+1}^{k} \frac{p_i - cr}{p_i - 1} = \prod_{i=a+1}^{k} \left(1 - \frac{cr-1}{p_i - 1}\right)$$

Ce rapport tend vers zéro car chacun de ses facteurs est inférieur à son correspondant dans la densité limite des nombres premiers jusqu'en p_k ; or cette dernière tend vers 0.

> La densité limite des nombres premiers liés par cr conditions en quantité finie est donc infiniment plus petite que la densité limite des nombres liés par $(cr-1)$ conditions.

III.4 Quelques applications

III.4.1 Caractérisation des nombres premiers

Ainsi que déjà vu au titre II, on peut écrire :

III.4.1.1 Ecriture en base 2

$$2q+1 \equiv \eta\, r_i \bmod 2p_i \quad \text{avec } r_i \neq p_i \quad \forall p_i < \left\lfloor \sqrt{2q+1} \right\rfloor$$

est l'écriture des nombres premiers selon le crible d'**Eratosthène,** ce qui s'écrit encore :

$$q \equiv r_i \bmod p_i \quad \text{avec} \quad r_i \neq i \quad \forall p_i = (2i+1) \leq \left\lfloor \sqrt{2q+1} \right\rfloor$$

où $2i+1$ est un nombre premier. Et la condition $r_i = i$ conduit bien à

$$2q+1 = (2k+1)(2i+1) \tag{3.7}$$

Un nombre $2q+1$ est donc premier si et seulement si chaque reste de sa division par chaque $p_i \leq \left\lfloor \sqrt{2q+1} \right\rfloor$ respecte une unique condition

III.4.1.2 Ecriture en base 6

$$6q + \varepsilon \neq (6k + \varepsilon\eta)\, p_i \qquad \forall \;\; p_i \leq \left\lfloor \sqrt{6q+1} \right\rfloor \tag{3.8}$$

Ainsi que nous l'avons montré précédemment (II.6.1à4), les sous-ensembles des nombres cadets premiers ($6q-1$) ou aînés premiers ($6q+1$) supérieurs à 3 se caractérisent par une condition et une seule sur le reste $r_{i\eta}$ de la division de leur paramètre q par chaque nombre premier $6i+\eta$ inférieur ou égal à $\left\lfloor \sqrt{6q+1} \right\rfloor$.

Si l'on a affaire aux cadets $6q-1$, ledit reste doit être différent de $-i\eta$:

$$q \equiv r_{i\eta} \bmod (6i+\eta) \quad r_{i\eta} \neq -i\eta \quad \forall \; (6i+\eta) \leq \left\lfloor \sqrt{6q-1} \right\rfloor \tag{3.9}$$

Si l'on a affaire à un aîné, ledit reste doit être différents de $+i\eta$.

$$q \equiv r_{i\eta} \bmod (6i+\eta) \quad r_{i\eta} \neq +i\eta \quad \forall \; (6i+\eta) \leq \left\lfloor \sqrt{6q+1} \right\rfloor \tag{3.10}$$

Ces deux relations sont bien équivalentes à $6q + \varepsilon \neq (6i+\eta)(6k+\varepsilon\eta)$ qui interdit le caractère composite de l'un ou l'autre des deux nombres $6q+\varepsilon$.

Donc toujours une seule condition pour chaque type de nombre premier cadet ou aîné.

III.4.2 Les nombres premiers et leur densité limite

Une seule condition les caractérise, d'où $cr = 1$, $p_{a+1} = 2$ et

$$N_k = (2-1)\times(3-1)\times\ldots.\times(p_k-1) \quad \text{dans chaque intervalle } \Pi_k = \prod_{i=3}^{k} p_i \tag{3.11}$$

La densité des paramètres q_{nk} et par conséquent celle des nombres premiers $2q_{nk}+1$, dans chaque intervalle Π_k,est donc :

$$\frac{N_k}{\Pi_k} = \prod_{j=1}^{k}\left(1-1/p_j\right)$$

Cette densité conduit au théorème de raréfaction de Legendre ; elle tend vers zéro, lorsque k augmente indéfiniment.

III.4.3 Les Polynômes producteurs de nombres premiers

Les polynômes ont fait l'objet de très nombreuses recherches: quels polynômes à coefficients entiers sont-ils susceptibles de produire une certaine quantité de nombres premiers et mieux en est-il qui puissent produire une infinité de nombres premiers ?

L'écriture générale d'un polynôme de degré b et d'indéterminée n est :

$$P(n) = a_n n^b + a_{n-1} n^{b-1} + ... + a_1 n + a_0$$

Afin de pouvoir produire des nombres premiers, une première condition est que $P(n)$ soit un polynôme primitif, c'est-à-dire que tous ses coefficients soient premiers les uns par rapport aux autres.

Il n'a jusqu'à présent pas été trouvé de polynômes de degré supérieur à 2 et qui soient capables de produire des nombres premiers pour une infinité de valeurs de n.

III.4.3.1 Les polynômes du premier degré et Dirichlet

Soit un polynôme $P(q) = a_1 q + a_0$; **Dirichlet** a démontré que si a_0 et a_1 sont premiers entre eux, alors il existe une infinité d'indéterminés q pour lesquels $P(q)$ est premier.

Supposons que $P(q) = a_1 q + a_0$ ne soit pas premier. Alors, il existe un entier q_i tel qu'au moins un nombre premier p_i soit un facteur de $P(q) = a_1 q_i + a_0$

$$P(q) = a_1 q_i + a_0 = (2k+1)\, p_i$$

D'où $$a_1 q_i \equiv (p_i - a_0)_i \bmod 2p_i$$

Ainsi, $P(q) = a_1 q + a_0$ sera premier si et seulement si le reste de la division de $a_1 q$ par $2p_i$ est différent de toute expression $p_i - a_0$

Une seule condition est imposée à q dans son parcours de 1 à l'infini.

L'expression a donc une infinité de valeurs premières selon la progression de q**.**

III.4.3.2 Les polynômes de degré supérieur à 1

Il est connu qu'au-delà du degré 2 aucun polynôme ne peut produire une quantité infinie de nombres premiers. Reste à le démontrer.