Arithmétique
(version chantier)

Marc SAGE

<2015

Table des matières

Albert Girard est le premier à donner l'expression générale de la formation des suites de Fibonacci. Il le fait dans sa traduction des cinquième et sixième livres de Diophante, en marge de l'édition de 1625 des œuvres de Simon Stevin. La veuve de Girard réédite cet énoncé en 1634, dans la publication de son œuvre posthume

th chinois : La première trace connue du problème figure dans le Sunzi suanjing (Classique mathématique de Maître Sun), composé entre le IIIe et le Ve siècle de notre ère ; d'où, probablement, le qualificatif de « chinois » dont on affuble, en Europe à partir des années 1850, le problème et le théorème qui le résout. Le voici, tel qu'exposé par Maître Sun (Sunzi) dans son « Classique », où il est le 26e problème du chapitre 3 :
source http ://www.math.ens.fr/culturemath/materiaux/irem-toulouse11/questions-sur-les-origines.html

D'où vient l'expression « modulo n » ?
Modulo est l'ablatif du mot latin modulus signifiant mesure ; modulo n signifie donc "à la mesure de n". L'expression a été introduite par Gauss en 1801.

calcul modulaire : rue pair-impair –> gen à 3 pour rues dans l'esapce (selon cone). Puis à 7 (jours de la semaine), 24 (heures), 60 (minutes).

finitude des nombres premiers : autre démo par le produit des $\sum_{k=0}^{N} \frac{1}{p^k} \leq \frac{1}{1-\frac{1}{p}}$. Le produit est $\geq \sum_{k=1}^{2^N} \frac{1}{k}$ car tout entier apparaît en développant. En regroupant les termes selon les puissance de $\frac{1}{2}$, ie $1 + \left(\frac{1}{2} + \frac{1}{3}\right) + \left(\frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7}\right) + ...$, on minore par $1 + \frac{N}{2}$, qui tend vers l'infini.
Répartition des premiers ? (cf JD page 102). En observant des tables, Gauss trouvait que le nombres de premiers entre x et $x + 1000$ était voisin de $\frac{1}{\ln x}$. D'où l'intutn, en intégrant (voir 1000 comme étant très petit) $\pi(x) \sim \int_2^x \frac{dt}{\ln t}$. C'est le th de Hadamard - De la Vallée Poussin.
Plus précis (JD page 104) : si $\pi(a, b, x)$ désigne le nombre de premiers situés dans la progression arhtihéti $an + b$, on montre que $\frac{\pi(a,b,x)}{\frac{x}{\ln x}} \longrightarrow \frac{1}{\varphi(\alpha)}$.

Commencer par la décomposition en premiers, pour voir les colonnes de premires (lemme de gauss et autrse) $\prod p^{v_p(\cdot)}$. Prolonger la v_p àQ, puis Legendre en exo + exo OMI $\frac{2a!2b!}{a!b!a+b!}$
ppremer => irred : $p = ab$ => a ou $b = 1$ (dans N)
a divise b ssi $v_p(a) \leq v_p(b)$ $\forall p$: corolooai : $a^2 \mid b^2$ ssi $a \mid b$
relation compatible avec produit : eg $p - 1 \mid k\frac{p-1}{2} \implies 2 \mid k \implies k$ pair
divisino eucli dans N avant Z (de tote façon elle a été faite en intro :-p)

Le pgcd et le ppcm de deux entiers a et b seront notés

$$\begin{cases} a \wedge b := \text{pgcd}(a, b) \\ a \vee b := \text{ppcm}(a, b) \end{cases}.$$

on lit d divise a et b
pgcd et ppcm sont définis comme des inf et sup pour la relation de divisaibilié, d'où leur associativité.
les introduire avec deux entiers, puis balanacer $\bigvee a_i$, puis sur Z en prenant les ||

$a \mid b \iff (b) \subset (a)$; pré-ordre : être associé $\iff |a| = |b|$.

utilie $a, b \mid n \implies \lambda a + \mu b \mid n$. Exemple : $\frac{a+b}{2} \wedge \frac{a-b}{2} = a \wedge b$
homogéeité : $\lambda a \wedge \lambda b = |\lambda| (a \wedge b)$

exemple : $n!+1$ et $(n+1)!+1$ sont premier entre eux. Un divisuer divise $(n+1)(n!+1) - ((n+1)! + 1) = n$, donc $n!$, donc la différence $(n! + 1) - n! = 1$.

L'algo d'Euclide est en fait ce qu'on fait à la main... $12 \wedge 33 = 12 \wedge 9 = 3 \wedge 9 = 3 \wedge 0 = 3$.
$a_0 = a$, $a_1 = b$, a_{n+1} =reste de a_n par $a_{n-1} = a_n - \left\lfloor \frac{a_n}{a_{n-1}} \right\rfloor a_{n-1}$, d'où $a_{n-1} \wedge a_n = a_n \wedge a_{n+1}$.Si $k = \min\{n, a_n = 0\}$, alors $a_k = a \wedge b$.
$12, 50, 15$ sont premiers entre eux, mais pas deux à deux.

Bézout 2 (le retour) $\sum(a_i) = (\bigwedge a_i)$
(on devrait dire Bachet-Bézout, 1621 dû à bachet de Méziriac, puis gén à $K[X]$ par Bézout)

équation $ax+by=c$: cas particulier, puis cas général (équation affine –> sol parituclière + solution linéaire)

exo : n prmier ssi (n) maximal , paraèle avec Z/nZ corps ssi n prmier :
inversible de Z/nZ, en profiter pour introduire $\varphi(n)$ et le th chinois.

division euclidienne : reste minimal ?

expo rapide : $a^{33} = \left(\left(\left(a^2\right)^2\right)^2\right)^2 \left(a^2\right)^2$etc... utilisé pour inverser dans Z/pZ par PTF

nombre de Mersenne : $2^N - 1$. Pour être premier, N doit être premier (sinon $N = ab$ et on factoiser $\left(2^a\right)^b - 1^b$). Quetino : y at-il infinité de Mersenne premiers ?
nombre de Fermat : $2^N + 1$. Pour être premier, N doit être une puissna de 2 (sinon $N = ai$ avec i impair et on peut facotoriser $\left(2^a\right)^i - (-1)^i$). Intérêt ? Un polygone régulier ayant un nombre premer p de côtés est contructible à la règle et au compas ssi p est de Fermat (3, 5, 17, 257, 65537, et après ?).

parler de RSA !
DES : commecner dans Z (puis n'importe quel anneau factorielle)

Dans tangente hors série, donner le critère de divisiblité par plein de trucs
Soit N écrit en base b dont on veut le reste modulo d. Soit n tq $N^n = 1\ [d]$ (existe si d premier, eg $d-1$ par PTF, mais très inefficace). On découpe N en tranches de n chiffres, mettons $N = N_k N_{k-1} ... N_0$. Alors $N - \sum N_i = \sum N_i b^{ni} = \sum N_i$.
EG ; en base $b = 10$, prenons $d = 3$ ou 9 : on retrouve critère classique (avec $n = 1$)
Pour $n = 2$, on a $10^2 - 1 = 99 = 3^2 \cdot 11$, pas pratique
Pour $n = 6$, on a $10^6 - 1 = 99999 = 3^2 \cdot 11 \cdot 41 \cdot 271$, donc div pr 41 ssi somm parquet de six chiffres l'est.
Vriante : si $N^n = -1\,[d]$, alors $d \mid N$ ssi $d \mid \sum(-1)^i N_i$.
EG : 11 !
En pratique, trouver n par diviion euclidiennt de b par d until un reste = 1.
EG : $7 \mid 10^3 + 1$, d'où critère avectranches de 3 chiffres
EG : $73 \mid 10^5 + 1$, d'où critère avectranches de 5 chiffres

Autre métohde : itérative, moins de calculs.
EG : si $N = Du = 10D + u$, alors $N = D - 2u\,[7]$
Plus général, si d divise $k10^n \pm 1$ $(k = 1, ..., 9)$, on tronque les n dernier chiffrs, on multiple cette tranche par k, puis on soustrait/additionne $(+1/-1)$ le résultat au nombre tronqué, et le carctère inversible du résultat reste le mêm modulo d.
Preuve : en écrivant $N = D10^n + U$, on a $10^n(D \pm kU) - N = (\pm k10^n - 1)D = 0$. Or 10^n est inversible mod d (d'inverse $\pm k$), d'où le résultat.
EG : 7 divise 21 et 399, donc on peut tronquer le dernier chiffres, le doubler, et soutraire le résultat (critère donné au début) ; ou bien tronquer les deux dernier chiffres, les multiplier par 4, et ajouter le résultat. Appiquer à 122456789 en mélangeant les deux.
EG : 13 dibise 91, donc coupe le dernier chiffrs, faire fois 9, et soutraire.
EG : 23 divise 299, donc on tronque les deux derniresr chiffrs, on ait fois 3, puis on additionne. Appiquer à
EG : $73 \mid 10^5 + 1$, d'où critère avectranches de 5 chiffres Appliquer à 123456746

0.1 Conjectures

catalan : prouvéé !

théorème de *Vinogradov* (tout entier impair assez grand est la somme de trois nombres premiers)
théorème de *Chen* (tout entier pair est la somme d'un premier et d'un produit d'au plus deux nombres premiers)

source *Additive Number Theory : The Classical Bases* de Melvyn B. Nathanson en GTM (chez Springer, donc), notamment la partie II (The Goldbach conjecture).

Syracuse

conjecture-abc

0.2 L'exo de dimitri au stage de préparation

Soit deux cercles de rayon $\frac{1}{2}$ posés sur la droite réelle aux abscisses 0 et 1. Ils sont donc tangents, donc engendrent un troisième cercle. On considère la plus petite famille de cercles contenant les deux premiers et stable par passage aux troisième cercle tangent. Décrire l'ensemble des abscisses de leurs centres.

Commençons par des calculs tout simples pour se familiariser avec ce fameux troisième cercle tangent.

Soit C_i deux cercles tangents de rayon r_i dont les centre ont pour abscisse $x_1 < x_2$. Notons r et x le rayon et l'abscisse du centre du troisième cercle tangent.
Pythagore donne $(x_2 - x_1)^2 + (r_2 - r_1)^2 = (r_1 + r_2)^2$, d'où

$$x_2 - x_1 = 2\sqrt{r_1 r_2}$$

(interprétation graphique par la moyenne géométrique ?).
On applique cela deux fois en télescopant un x :

$$x_2 - x_1 = (x_2 - x) + (x - x_1) = 2\sqrt{r}\left(\sqrt{r_2} + \sqrt{r_1}\right).$$

On en déduit

$$r = \left(\frac{\sqrt{r_1 r_2}}{\sqrt{r_1} + \sqrt{r_2}}\right)^2 = \frac{1}{\left(\frac{1}{\sqrt{r_1}} + \frac{1}{\sqrt{r_2}}\right)^2} = \frac{1}{4} M_{-\frac{1}{2}}(r_1, r_2).$$

Puis les quotients donnent $\frac{x - x_1}{x_2 - x} = \sqrt{\frac{r_1}{r_2}}$, d'où

$$x = \frac{\sqrt{\frac{r_1}{r_2}} x_2 + x_1}{\sqrt{\frac{r_1}{r_2}} + 1} = \text{bar} \begin{array}{cc} x_1 & x_2 \\ \frac{1}{\sqrt{r_1}} & \frac{1}{\sqrt{r_2}} \end{array}.$$

Un récurrence immédiate montre que le n-ième cercle de gauche a pour rayon $\frac{1}{2n^2}$ et pour abscisse $\frac{1}{n}$. On peut généraliser cela à condition de bien voir comment "généraliser" le n ci-dessus à d'autrse cercles.
Associons un numéro à chacune des cercles de la sorte : 1 pour les deux premiers, puis le numéro d'un troisième cercle tangent s'obtient en sommant les numéros des cercles parents.

Montrons alors qu'un cercle numéroté n a pour rayon $\frac{1}{2n^2}$.
Pour $n = 1$, c'est l'hypothèse de départ.
Supposons le résultat montrer jusqu'à un rang $n - 1 \geq 1$. Un cercle n s'obtient en recollant deux cercles k et $n - k$ pour un certain k entre 1 et $n - 1$, d'où le rayon du cercle n :

$$r = \frac{1}{\left(\sqrt{2}\,|k| + \sqrt{2}\,|n - k|\right)^2} = \frac{1}{2n^2}.$$

Montrons ensuite par récurrence sur les numéros $n \geq 1$ qu'il y a un a premier avec n tel que le centre du cercle considéré soit d'abscisse $\frac{a}{n}$.
Pour $n = 1$, il n'y a rien à faire.
Supposons le résultat montré pour $1, ..., n - 1 \geq 1$. On obtient un cercle n en touchant deux cercles p et q avec $1 \leq p, q$ tels que $p + q = n$, d'où $p, q < n$ et par récurrence un $a \wedge p = 1$ et un $b \wedge q = 1$ tels que $\begin{cases} x_p = \frac{a}{p} \\ x_q = \frac{b}{q} \end{cases}$.
On en déduit

$$x_n = \text{bar} \begin{array}{cc} \frac{a}{p} & \frac{b}{q} \\ \sqrt{2p} & \sqrt{2q} \end{array} = \frac{a + b}{n}.$$

Par ailleurs, on a

$$\begin{aligned} |x_q - x_q| &= 2\sqrt{\frac{1}{2q^2}\frac{1}{2p^2}} \\ \left|\frac{aq-bp}{pq}\right| &= \frac{1}{pq} \\ |q\,(a+b) - b\,(p+q)| &= 1 \\ n \wedge (a+b) &= 1, \text{ CQFD.} \end{aligned}$$

La création d'un cercle tangent à deux autres préexistant se traduit par $\{a,b\} \mapsto \{\max, \min + \max\}$, l'opération inverse s'effectuant par $\{a,b\} \mapsto \{\min, \max - \min\}$. Ainsi, si l'on part de deux cercles tangents, le procédé montant va s'arrêter (nécessairement car le max décroît) et ce uniquement lorsque l'on arrivera au singleton $\{1,1\}$ conrrepondant aux cercles de départ. Mais à chaque étape on fait des combinaison linéaires des précédents éléments. Il y a donc une telle combinaison valant 1, d'où $a \wedge b = 1$.

Montrons réciproquement que pour deux entiers $a \wedge b = 1$ on peut trouver deux cercles a et b tangents. Par récurrence sur $a + b$.

Pour $(a,b) = (1,1)$, ce sont les cercles de départ.

Pour $(a,b) \neq (1,1)$, on a déjà $a \neq b$: sinon $a = b$ qui ne peut valoir 1, mais alors $a \wedge b = a = b \neq 1$. Supposons $a < b$ par symétrie. Alors nos deux cercles devraient provenir de cercles a et $b - a$, dont la somme b est $< a + b$ et tels que $a \wedge (b - a) = a \wedge b = 1$. L'hypothèse de récurrence nous fournit de tels cercles, CQFD.

Ainsi, pour aboutir à un cercle n, il faut partir de cercles p et q se touchant (avec $p + q = n$), donc tels que $1 = p \wedge q = p \wedge n$. Il y a donc au moins autant de cercles n que de paires $\{p,q\}$ distinctes vérifiant $p + q = n$ et $p \wedge n = 1$, donc au moins autant que d'entiers $p < \frac{n}{2}$ tels que $p \wedge n = 1$. Or, chaque telle paire de cercles apparaît à deux reprises (au moins) à cause de la symétrie par rapport à $\frac{1}{2}$. On obtient ainsi autant de cercles que d'entiers $\neq \frac{n}{2}$ étrangers à n. Quand à la fraction $\frac{1}{2}$, étant sous forme irréductible, elle n'est atteinte que pour $n = 2$. Ainsi, pour $n \geq 3$, il y a (au moins) autant de cercles n que d'entiers $< n$ étrangers à n, çàd autant que de de fractions irréductibles $\frac{a}{n}$ où $1 \leq a < n$. YOUPI !