Entrelacs premiers (Denise Vella-Chemla, 4.5.2016)

On étudie la manière dont le théorème de Wilson permet de lier les nombres premiers à certaines permutations.

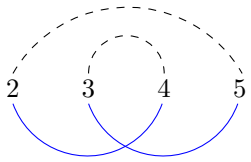
Le théorème de Wilson énonce que p est un nombre premier si et seulement si $(p-1)! \equiv -1 \ (mod\ p)$. Comme $p-1 \equiv -1 \ (mod\ p)$, cela équivaut à $(p-2)! \equiv 1 \ (mod\ p)$. Les nombres de 2 à $p-2$ (au nombre de $p-3$) peuvent être regroupés par 2 lorsque leur produit est congru à l'unité selon le module p (cf en annexe les articles 75 à 78 des Recherches arithmétiques de Gauss).

Illustrons sur quelques dessins la symétrie des *"entrelacs premiers"* découlant de ce théorème.

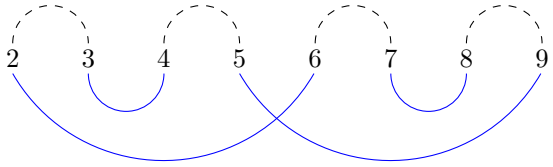
Selon le module 7 premier,

$$2.4 \equiv 8 \equiv 1 \ (mod\ 7)$$
$$3.5 \equiv 15 \equiv 1 \ (mod\ 7)$$

On lie les nombres 2 et 4 d'une part, 3 et 5 d'autre part, par des liens bleus, on complète le schéma par des liens pointillés pour fermer l'entrelacs (les liens bleus représentent ainsi des propositions logiques vraies (i.e. un lien bleu entre x et y représente la proposition $xy \equiv 1 \ (mod\ p)$) et les liens pointillés représentent des propositions logiques fausses). L'entrelacs obtenu est dénommé *entrelacs de Hopf*[1].

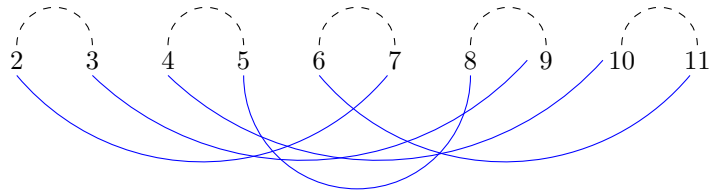


Selon le module 11 premier



[1]Maryam Mirzakhani trace au tableau des dessins similaires, lors d'un cours visionnable sur la toile, à la minute 2 derrière ce lien : *Dynamics of the moduli spaces of curves*. Les lignes ne se croisent pas dans le problème qu'elle présente.

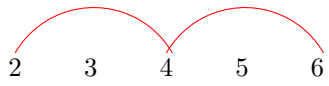
Selon le module 13 premier



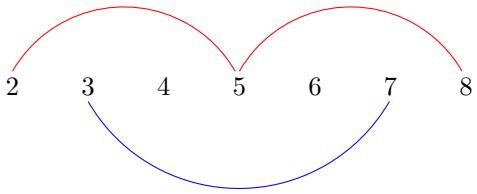
Les symétries autour de l'axe vertical passant par $p/2$ sont dûes au fait que $(p-x)(p-y) \equiv xy \ (mod\ p)$.

Selon les modules composés, tout nombre n'admet pas forcément un inverse dans $\mathbb{Z}/p\mathbb{Z}$. Dans $\mathbb{Z}/10\mathbb{Z}$ et $\mathbb{Z}/15\mathbb{Z}$, on trouve des paires de nombres dont le produit est congru à l'unité (notées par des liens bleus) mais on ne trouve pas systématiquement une telle paire de nombres (cf le module 8). Pour les modules composés, on note en rouge ci-dessous les paires de nombres dont le produit est congru à 0 selon le module considéré.

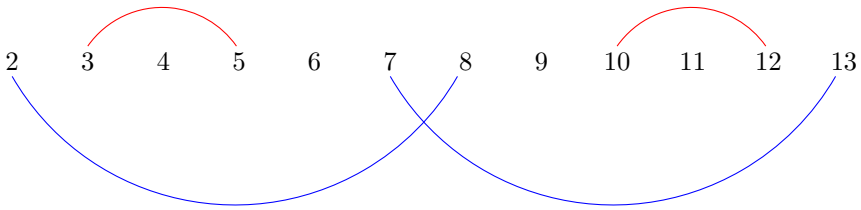
Selon le module 8 composé



Selon le module 10,



Selon le module 15,



On peut utiliser ces constatations pour associer à chaque nombre premier une permutation : elle envoie chaque nombre sur son inverse et on "complète les

trous" pour fermer l'entrelacs.

Ainsi la permutation que l'on associe au nombre premier 7 est

$$\begin{pmatrix} 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 \end{pmatrix}$$

et celle que l'on associe au nombre premier 11 est

$$\begin{pmatrix} 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 2 & 3 & 4 & 7 & 8 & 9 & 5 \end{pmatrix}.$$

On peut du même coup associer à chaque nombre premier p une matrice de permutation, moyennant un renommage des nombres de 2 à $p-2$ en leur prédécesseur de 1 à $p-3$; c'est une matrice carrée de taille $(p-3)\times(p-3)$. Celle associée au nombre premier 7 est

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

et celle associée au nombre premier 11[2] est

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Il faudrait chercher une opération sur les matrices de permutation que l'on pourrait mettre en correspondance avec la multiplication habituelle.

[2]Le renommage s'effectue ainsi (résultat en bleu) :

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 2 & 3 & 4 & 7 & 8 & 9 & 5 \\ 5 & 1 & 2 & 3 & 6 & 7 & 8 & 4 \end{array}$$

;

Annexe 1 : Articles 75 à 78 des Recherches arithmétiques de Carl-Friedrich Gauss

75. Avant d'abandonner ce sujet, nous présenterons quelques propositions qui ne nous paraissent pas indignes d'attention, à cause de leur simplicité.
Le produit de tous les termes de la période d'un nombre quelconque est $\equiv 1$ *quand leur nombre ou l'exposant auquel appartient le nombre dont il s'agit est impair, et* $\equiv -1$ *quand il est pair.*
Par exemple, pour le module 13, la période de 5 est composée des termes $1, 5, 12, 8$ dont le produit $480 \equiv -1$ (*mod* 13), suivant le même module, la période de 3 est composée des termes $1, 3, 9$, dont le produit $27 \equiv 1$ (*mod* 13).
Soit t l'exposant auquel le nombre appartient ; on peut toujours trouver (n°71) une base pour laquelle l'indice du nombre soit $\frac{p-1}{t}$. Or l'indice du produit de tous les termes sera

$$(1 + 2 + 3 + etc. + t - 1)\frac{p-1}{t} = \frac{(t-1)(p-1)}{2};$$

donc il sera $\equiv 0$ (*mod* $p-1$), quand t est impair et $\equiv \frac{p-1}{2}$ quand t est pair. Dans le premier cas, le produit est $\equiv 1$ (*mod* p) ; dans le second, $\equiv -1$ (*mod* p).

76. Si le produit du théorème précédent est une racine primitive, sa période comprendra tous les nombres $1, 2, 3, 4, \ldots p-1$, dont le produit sera par conséquent toujours $\equiv -1$; car $p-1$ est toujours pair, excepté dans le cas où $p = 2$, et alors on a indifféremment $+1$ ou -1. Ce théorème élégant qu'on énonce ordinairement de cette manière : *Le produit de tous les nombres plus petits qu'un nombre premier étant augmenté de l'unité, est divisible par ce nombre premier,* a été publié par *Waring* qui l'attribue à *Wilson* (*Meditationes Algeb. Ed. 3, p. 380*) ; mais aucun des deux n'a pu le démontrer, et *Waring* avoue que la démonstration lui en semble d'autant plus difficile qu'il n'y a point de *notation* par laquelle on puisse exprimer un nombre premier ; pour nous, nous pensons que la démonstration de cette sorte de vérités doit être puisé dans les principes plutôt que dans la notation. *Lagrange* en a depuis donné une démonstration (*Nouv. Mém. de l'Ac. de Berlin, 1771)*, dans laquelle il s'appuie sur la considération des coefficients que l'on trouve en développant le produit

$$(x+1)(x+2)(x+3)\ldots(x+p-1) :$$

et il fait voir qu'en supposant ce produit

$$= x^{p-1} + Ax^{p-2} + Bx^{p-3} + etc. + Mx + N,$$

les coefficients A, B, etc. M sont divisibles par p ; or

$$N = 1.2.3\ldots p-1$$

Maintenant si $x = 1$, le produit est divisible par p, mais alors il sera $\equiv 1 + N$ (*mod* p) donc $1 + N$ est divisible par p.
Enfin Euler *(Opusc. analyt. T.1, p.329)* en a donné une démonstration qui rentre dans celle que nous venons d'exposer ; ainsi puisque de tels hommes n'ont

pas cru ce sujet indigne de leurs méditations, nous espérons qu'on ne nous désapprouvera pas d'offrir encore ici une autre manière de démontrer ce théorème.

77. Nous dirons que deux nombres sont *associés*, comme l'a fait *Euler*, lorsque leur produit sera congru à l'unité. Cela posé, par la section précédente, tout nombre positif moindre que p, aura toujours un nombre associé moindre que p et il n'en aura qu'un ; or il est facile de prouver que parmi les nombres $1, 2, 3, -1$, il n'y a que 1 et $p-1$ qui soient eux-mêmes leurs associés, car ceux qui jouiront de cette propriété seront donnés par la congruence $x^2 \equiv 1$ qui ne peut avoir que 2 racines 1 et $p-1$. Supprimant donc ces deux nombres, les autres $2, 3, 4 \ldots p-2$, seront associés deux à deux, donc leur produit sera $\equiv 1$; enfin multipliant par $p-1$, le produit de tous $1.2.3.4 \ldots p-1 \equiv p-1 \equiv -1$.
Par exemple, pour $p = 13$, les nombres $2, 3, 4, 5, \ldots 11$ s'associent de la manière suivante : 2 avec 7, 3 avec 9, 4 avec 10, 5 avec 8, 6 avec 11 ; donc $2.3.4 \ldots 11 \equiv 1$, et partant..... $1.2.3 \ldots 12 \equiv 12 \equiv -1$.

78. Le théorème de *Wilson* peut être rendu plus général en l'énonçant comme il suit : *Le produit de tous les nombres premiers avec un nombre donné A et moindres que ce nombre, est congru suivant A, à l'unité prise positivement ou négativement.* L'unité doit être prise négativement quand A est de la forme p^m ou $2p^m$, p étant un nombre premier différent de 2, ou encore quand $A = 4$; et positivement dans tous les autres cas. Le théorème de Wilson est contenu dans le premier cas. *Exemple.* Pour $A = 15$, le produit des nombres $1, 2, 4, 7, 8, 11, 13, 14$ est $\equiv 1$ (*mod* 15). Nous supprimons, pour abréger, la démonstration. Nous observerons seulement qu'on peut y parvenir comme dans l'article précédent, excepté que la congruence $x^2 \equiv 1$ peut avoir plus de 2 racines, ce qui demande certaines considérations particulières. On pourrait aussi la tirer de la considération des indices, comme dans le n°75, si l'on y joint ce que nous dirons tout à l'heure des modules composés.

Annexe 2 : Article 41 des Recherches arithmétiques de Carl-Friedrich Gauss

Dans l'article 41 des Recherches arithmétiques de Gauss, on retrouve la notion de permutations et on pense aux travaux de Galois à venir.

41. *Si p est un nombre premier, et qu'on ait p choses parmi lesquelles il peut s'en trouver un certain nombre d'égales entre elles, pourvu que toutes ne le soient pas : le nombre des permutations de ces choses sera divisible par p.*

Par exemple, cinq choses A, A, A, B, B peuvent se disposer de dix manières différentes.

La démonstration de ce théorème se déduit facilement de la théorie connue des permutations. En effet, supposons que parmi ces p choses, il y en ait a égales à A, b égales à B, c égales à C etc., de sorte qu'on ait $a + b + c + etc = p$, les nombres a, b, c,etc. pouvant aussi désigner l'unité. Le nombre de permutations sera $= \dfrac{1.2.3 \ldots p}{1.2 \ldots a.1.2 \ldots b.1.2 \ldots c.etc.}$; or le numérateur est évidemment divisible

par le dénominateur, puisque le nombre des permutations est entier ; mais il est divisible par p, tandis que le dénominateur, qui est composé de facteurs plus petits que p, n'est pas divisible par p (n°15) ; donc le nombre des permutations sera divisible par p.

Nous espérons cependant que la démonstration suivante ne déplaira pas à quelques lecteurs.

Lorsque dans deux permutations l'ordre des choses ne différera qu'en ce que celle qui tient la première place dans l'une, en occupe une différente dans l'autre, mais que du reste toutes les autres choses, à partir de celle-là, suivent le même ordre dans chacune des permutations, de manière que la dernière de l'une se trouve placée immédiatement avant la première, dans l'autre ; nous les appellerons permutations semblables[3]. Ainsi $ABCDE$ et $DEABC$, $ABAAB$ et $ABABA$ seront semblables.

Or comme chaque permutation est composée de p choses, il est clair qu'on pourra en trouver $p-1$ semblables à une quelconque d'entre elles, si l'on met successivement à la seconde, à la troisième place, etc., la chose qui occupait la première ; donc si aucunes de ces permutations semblables ne sont identiques, il est évident que le nombre total des permutations sera égal à p fois le nombre des permutations dissemblables, et conséquemment sera divisible par p. Supposons que deux permutations semblables $PQ\dots TV\dots, V\dots YZPQ\dots T$ puissent être identiques, et que P qui occupe la première place dans la première, occupe la $n+1^{ième}$ dans la seconde : on aura dans la dernière série le $n+1^{ième}$ terme égal au 1^{er}, le $n+2^{ième}$ égal au $2^{ième}$, etc., d'où résulte que le $2n+1^{ième}$ est encore égal au premier et par conséquent le $3n+1^{ième}$, et généralement le $kn+m^{ième}$ égal au $m^{ième}$ (où quand $kn=m>p$, il faut imaginer qu'on reprenne toujours par le commencement, la série $V\dots T$, à moins qu'on ne retranche de $kn+m$, le multiple de p, qui en approche le plus en moins). Cela posé, si on détermine k de manière que $kn\equiv 1\ (mod\ p)$, ce qui peut toujours se faire, puisque p est premier, il suivra de là que généralement le $m^{ième}$ terme serait égal au $m+1^{ième}$, c'est à dire qu'un terme quelconque serait égal au suivant, ou que tous les termes seraient égaux entre eux, ce qui est contre l'hypothèse.

[3]Si l'on écrivait en cercle les permutations semblables, de manière que la dernière chose touchât la première, il n'y aurait aucune différence entre elles, parce qu'aucune place ne peut s'appeler la première ni la dernière.