Une preuve géométrique du théorème de Wilson.

Écrit par
Dr. K. Petr.

Le théorème de Wilson nous dit que le nombre $1.2.3\ldots(p-1)+1$ (ou autrement, écrit $(p-1)!+1$) est divisible par p, si p est premier. Pour prouver ce théorème, imaginons dans le plan les p points $A_1, A_2, \ldots, A_p$ sommets d'un polygone régulier et considérons d'abord de combien de façons il est possible de connecter ces p points avec une ligne brisée constituée de p segments ayant ces points comme extrémités. Il y a probablement autant de façons qu'il y a de permutations de $p-1$ éléments différents, c'est-à-dire qu'il y en a $(p-1)!$ parce qu'à partir d'un point, par exemple du point A_x, on peut parcourir le reste des points dans n'importe quel ordre. Ce faisant, nous considérons deux lignes qui se chevauchent mais qui vont dans la direction opposée comme différentes. Ces lignes brisées fermées sont de deux types, les régulières ou les irrégulières. Les régulières sont celles qui, si on les fait tourner autour du centre correspondant aux points $A_1, A_2, \ldots, A_p$ d'un angle $\dfrac{2\pi}{p}$ ou par des multiples de cet angle $\dfrac{2\pi}{p}, \dfrac{4\pi}{p}, \ldots, \dfrac{2(p-1)\pi}{p}$, vont se recouvrir elles-mêmes. Les irrégulières ont alors la propriété que si nous faisons tourner les points $A_1, A_2, \ldots, A_p$, de n'importe lequel des angles, nous obtenons une ligne brisée, reliant les points mais dans un ordre différent de celui dont nous sommes partis. Par conséquent, les lignes discontinues irrégulières peuvent être assemblées en groupes de p membres chacun. D'une ligne brisée irrégulière, on obtient toutes les autres du même groupe, si l'on fait tourner cette ligne brisée autour du centre d'angles successifs

$$\frac{2\pi}{p}, \frac{4\pi}{p}, \ldots, \frac{p-1}{p}2\pi$$

Il n'y a pas d'autres lignes brisées. Car supposons que nous ayons une ligne brisée qui se couvrirait si nous la tournions autour du centre q d'un angle $q\dfrac{2\pi}{p}$, et supposons que q serait le plus petit nombre ayant cette propriété $\quad (1 < q < p)$.

Alors, cette ligne se couvrirait également lorsqu'on la tournerait d'un angle égal à

$$\frac{2.q2\pi}{p}, \quad \frac{3.q2\pi}{p}, \ldots, \frac{\lambda.q2\pi}{p}.$$

Soit λ un entier tel que

$$(\lambda-1)q < p \quad \text{et} \quad \lambda q > p,$$

Retranscription en Latex et correction de la traduction par Google : Denise Vella-Chemla, août 2022.

alors

$$\lambda q = p + q_1,$$

où, puisque p est premier

$$0 < q_1 < q \ ;$$

et la ligne brisée se chevaucherait à l'angle

$$\frac{\lambda . q 2\pi}{p} = 2\pi + \frac{q_1 2\pi}{p}$$

c'est-à-dire à un angle $\frac{q_1 2\pi}{p}$, ce qui est contraire à l'hypothèse que q est le plus petit nombre ayant cette propriété.

Il y a $p - 1$ lignes brisées régulières, car une ligne brisée régulière est complètement définie par une ligne de connexion, et nous pouvons relier le point 1 par exemple avec seulement $(p - 1)$ points différents. Soit N le nombre de groupes à p éléments de lignes brisées irrégulières. Alors on a

$$(p - 1)! = p - 1 + Np$$

ou

$$(p - 1)! + 1 = p(N + 1)$$

ce qui prouve le théorème de Wilson.