36.
Démonstrations nouvelles de quelques théorèmes relatifs aux nombres.

(Par Mr. *Lejeune-Dirichlet*, prof. de mathém.)

Parmi les différentes démonstrations que les géomètres ont successivement données du théorème de Wilson, celle que M. Gauss a exposée dans ses "*Disquisitiones arithmeticae*, art. 77." et qui est fondée sur la considération des nombres correspondants (*numeri socii*) est sans contredit la plus simple. En généralisant un peu la définition des nombres correspondants et en suivant ensuite une marche analogue à celle de M. Gauss, on peut démontrer simultanément le théorème de Wilson et deux autres propositions qui sont d'un grand usage dans la théorie des nombres. C'est ce que nous allons faire voir en peu de mots.

La lettre p désignant un nombre premier, Euler qui le premier s'est servi de cette considération, nomme *correspondants* deux nombres m et n l'un et l'autre moindres que p et tels que leur produit mn donne l'unité pour reste lorsqu'il est divisé par p.

Généralisons cette définition et appelons correspondants deux nombres m et n moindres que p et dont le produit mn donne le même reste qu'un nombre déterminé a que nous supposons n'être pas divisible par p. Cela posé, considérons la suite

$$(1.) \qquad 1, 2, 3, ...p-1.$$

Il est facile de voir que, si m désigne l'un quelconque des nombres qui composent cette suite, ce nombre m aura son correspondant n et n'en aura qu'un. Cela résulte immédiatement de ce que la congruence $my \equiv a \pmod{p}$ dans laquelle ni m ni a n'est divisible par p, a toujours une racine y moindre que p et n'en a qu'une.

Il peut arriver que n soit égal à m. On a alors $m^2 \equiv a \pmod{p}$, ce qui fait voir que ce cas ne peut avoir lieu qu'autant qu'il existe un carré donnant le même reste que a, ou, en d'autres termes, qu'autant que a est résidu quadratique par rapport à p. Distinguons actuellement deux cas selon que a est ou n'est pas résidu quadratique par rapport à p et commençons par le dernier de ces deux cas.

Soit, dans ce cas, m l'un quelconque des nombres (1.) et n son correspondant. On aura $mn \equiv a \pmod{p}$ et n sera différent de m. Après avoir oté les nombres m, n de la suite (1.), il restera $p-3$ nombres. Désignons par m' l'un quelconque de ces $p-3$ nombres restants et par n' son correspondant ; n' sera différent de m' et l'on aura $m'n' \equiv a \pmod{p}$ En continuant de procéder ainsi, ou épuisera la suite (1.) et l'on formera $\frac{p-1}{2}$ groupes composés chacun de 2 nombres correspondants ; car chaque nombre n'ayant qu'un correspondant qui est mis de côté en même temps que lui, on ne peut jamais, pour former un nouveau groupe, avoir besoin d'un des nombres déjà mis de côté.

Référence : Journal für die reine und angewandte Mathematik (Journal de Crelle), Volume 1828, Issue 3, page 390.

Le produit de deux nombres composant un groupe donnant le même reste que a, et les groupes étant au nombre de $\frac{p-1}{2}$, on voit que le produit des nombres dont l'ensemble des groupes est formé, c'est-à-dire le produit des nombres compris dans la série (1.) donne le même reste que le nombre a élevé à la puissance $\frac{p-1}{2}$. On a donc dans le cas que nous venons d'examiner

$$(2.) \qquad 1.2.3...p-1 = a^{\frac{p-1}{2}} \text{ (mod. } p).$$

Passons au second cas qui a lieu lorsque a est résidu quadratique de p. Il existe dans ce cas un carré k^2 (dont la racine k peut être supposée $< p$) tel que $k^2 \equiv a$ (mod. p). Le carré du nombre $p-k$, qui est également moindre que p, donne aussi le même reste que a lorsqu'il est divisé par p. Les nombres k et pk étant otés de la suite (1.), il n'y restera aucun nombre x tel que $x^2 \equiv a$ (mod. p). Car si parmi les nombres restants il y en avait un satisfaisant à cette condition, $x^2 - k^2 = (x+k)(x-k)$ serait divisible par p ; il faudrait donc qu'un des facteurs $x+k, x-k$ le fut pareillement ; or c'est ce qui est manifestement impossible, x étant plus petit que p et différent de k et $p-k$. Cela posé, on voit comme dans le cas déjà examiné, que les $p-3$ nombres qui restent dans la suite (1.) après en avoir oté k et $p-k$, se correspondent deux à deux, d'où l'on conclut comme précédemment que le produit de ces nombres donne le même reste que $a^{\frac{p-3}{2}}$. Il suit de là que le produit de tous les nombres qui composent la suite (1.) donne le même reste que $a^{\frac{p-3}{2}} k(p-k)$ et comme, d'après ce qu'on a vu plus haut, on a $k(p-k) = -k^2 \equiv -a$ (mod p), il vient ce résultat

$$1.2.3....p-1 = -a^{\frac{p-1}{2}} \text{ (mod. } p).$$

Ce résultat et celui que nous avons obtenu plus haut, peuvent être réunis dans la formule suivante

$$(3.) \qquad 1.2.3....p-1 = \mp a^{\frac{p-1}{2}} \text{ (mod. } p)$$

dans laquelle il faut prendre le signe supérieur ou inférieur, selon que le nombre a que nous supposons n'être pas divisible par p, est ou n'est pas résidu quadratique de p. Si nous posons $a = 1$, le signe supérieur aura lieu, l'unité étant un carré et par conséquent résidu quadratique de tout nombre. Nous avons donc

$$1.2.3....p-1 \equiv -1 \text{ (mod. } p)$$

congruence qui constitue le théorème de Wilson.

Remplaçons le premier membre de la formule (3.) par le nombre -1, qui comme nous venons de le voir, n'en diffère que d'un multiple de p, et changeons ensuite les signes des deux membres ; il viendra ainsi

$$a^{\frac{p-1}{2}} = \pm 1 \text{ (mod. } p)$$

congruence dans laquelle il faudra choisir le signe $+$ ou le signe $-$, selon que a est ou n'est pas résidu quadratique de p. Le théorème que cette formule renferme, et qui a été découvert par Euler, est d'une grande importance dans la théorie des résidus. On fera disparaître le double signe dans la dernière congruence en élevant ses deux nombres au carré. On trouve ainsi

$$a^{p-1} \equiv 1 \text{ (mod. } p)$$

ce qui est le théorème de Fermat.

Ce dernier théorème peut être démontré très simplement de la manière suivante, sans qu'il soit nécessaire de rien supposer de ce qui précède.

Les nombres a et p conservant leur signification, considérons les $p-1$ multiples de a que voici :

$$a, 2a, 3a, \ldots, (p-1)a.$$

Il est facile de voir que deux de ces nombres ne sauraient donner le même reste quand on les divise par p ; car si les restes provenant des multiples ma et na étaient égaux, $ma - na = (m-n)a$ serait divisible par p, ce qui est impossible, a n'étant pas divisible par p, et $m-n$ étant $< p$ sans pouvoir être zéro. Les restes que l'on obtient en divisant par p les $p-1$ multiples de a, étant tous différents entre eux et aucun de ces restes ne pouvant être nul, comme on le voit facilement, ces restes doivent coïncider avec les nombres de la série $1, 2, 3, ..., p-1$, quand on fait abstraction de l'ordre dans lequel ils se suivent. Il suit de là que le produit des $p-1$ multiples de a, doit donner le même reste que le produit $1.2.3...p-1$.

La différence de ces produits est donc un multiple de p. Or cette différence pouvant facilement se mettre sous la forme

$$(a^{p-1} - 1)(1.2.3....p-1)$$

et $1.2.3...p-1$ n'étant pas divisible par p, on en conclut que $a^{p-1} - 1$ est multiple de p, ou, ce qui est la même chose, que a^{p-1} étant divisé par p donne l'unité pour reste.