36.

SUR UNE PROPRIÉTÉ DES NOMBRES PREMIERS QUI SE RATTACHE AU THÉORÈME DE FERMAT.

[*Comptes Rendus de l'Académie des Sciences*, LII. (1861), pp. 161—163.]

En étudiant les propriétés arithmétiques des nombres de Bernoulli et des autres nombres qui leur sont analogues, je suis tombé tout récemment sur une représentation du résidu par rapport au module p^2 de la même fonction exponentielle r^{p-1} dont le théorème de Fermat enseigne que le résidu par rapport à p est l'unité. Nommons le nombre entier $\frac{r^{p-1}-1}{p}$ le quotient de Fermat, dont p sera dit le module et r la base. En supposant que la base est un nombre premier, je trouve qu'on peut exprimer son résidu par rapport au module au moyen d'une série de fractions dont les dénominateurs seront tous les nombres inférieurs au module p, et les numérateurs des nombres périodiques qui ne dépendent que de la base r.

En effet, si le module est un nombre premier impair, les fractions qui expriment ce résidu auront pour dénominateurs successifs $p-1$, $p-2$, $p-3, \ldots, 2, 1$, et pour numérateurs* le cycle toujours répété $1, 2, 3, \ldots, r-1, r$, sauf à entendre que le cycle des numérateurs commence avec le terme qui est congru à $\frac{1}{p}$ par rapport à r. Par exemple, soit $r=5$, nous aurons d'après cette règle

$$\frac{5^{p-1}-1}{p} \equiv \frac{1}{p-1}+\frac{2}{p-2}+\frac{3}{p-3}+\frac{4}{p-4}+\frac{5}{p-5}+\frac{1}{p-6}+\frac{2}{p-7}+\ldots,$$

quand p est de la forme $10k+1$, mais* [à cause de $2\times 3 \equiv 1 \pmod 5$]

$$\equiv \frac{3}{p-1}+\frac{4}{p-2}+\frac{5}{p-3}+\frac{1}{p-4}+\frac{2}{p-5}+\ldots,$$

quand p est de la forme $10k+2$. Il est bon de remarquer que la somme des réciproques des dénominateurs étant congrue à zéro pour le module p, on peut augmenter ou diminuer simultanément (à volonté) tous les termes

[* See correction below, p. 241.]

du cycle d'un même nombre quelconque, et conséquemment pour le cycle 1, 2, 3, ..., r, on peut substituer un cycle plus symétrique dans lequel le terme au milieu sera zéro. Ainsi on trouve en prenant $r=3$ (suivant le module p)

$$\frac{3^{p-1}-1}{p} \equiv -\frac{1}{p-1}+\frac{1}{p-3}-\frac{1}{p-4}+\frac{1}{p-6}-\frac{1}{p-7}\cdots,$$

ou

$$\equiv -\frac{1}{p-2}+\frac{1}{p-3}-\frac{1}{p-5}+\frac{1}{p-6}\cdots,$$

selon que p est de la forme $6n+1$ ou $6n-1$ respectivement.

Par exemple, faisons $p=7$, alors

$$-\frac{1}{6}+\frac{1}{4}-\frac{1}{3}+\frac{1}{1} \equiv -6+2-5+1 \equiv 6 \equiv \frac{3^6-1}{7}$$

c'est-à-dire $\equiv 104 \pmod 7$.

Prenons encore $p=11$, alors

$$\frac{1}{9}-\frac{1}{8}+\frac{1}{6}-\frac{1}{5}+\frac{1}{3}-\frac{1}{2} \equiv 5-7+2-9+4-6 \equiv 0 \equiv \frac{3^{10}-1}{11}$$

c'est-à-dire $\equiv 22 \times (3^5+1) \pmod{11}$.

Reste à donner la série pour le cas où la base du quotient de Fermat est le nombre 2 [cf. p. 235 below]. Par ce cas on trouve

$$\frac{2^{p-1}-1}{p} \equiv \frac{2}{p-3}+\frac{2}{p-4}+\frac{2}{p-7}+\frac{2}{p-8}+\frac{2}{p-11}+\cdots,$$

ou*

$$\equiv \frac{2}{p-2}+\frac{2}{p-3}+\frac{2}{p-6}+\frac{2}{p-7}+\frac{2}{p-10}+\cdots,$$

selon que p est de la forme $4k+1$ ou $4k-1$ respectivement. On peut énoncer des théorèmes plus généraux en substituant pour p et $p-1$ un nombre quelconque et un indicateur maximum respectivement. Pour le moment je me borne à faire une remarque sur la constitution arithmétique des nombres de Bernoulli et des nombres analogues qui entrent dans le développement des sécantes, dont l'étude m'a conduit à la loi donnée plus haut. Quant aux nombres de Bernoulli, on sait déjà par le théorème publié presque simultanément par MM. Clausen et Staudt, que le dénominateur de B_n est un produit de puissances simples de nombres premiers, étant composé du produit de tous les nombres premiers qui, diminués par l'unité, sont diviseurs de $2n$. Mais on paraît ne pas avoir fait la remarque importante que le numérateur de B_n contiendra tous les facteurs de n qui ne sont pas puissances des facteurs du dénominateur, de telle sorte que, si n contient

[* The sign of every term in the second expression should be changed. Stern, *Crelle*, Bd c. (1887), p. 188.]

p^i, mais ne contient pas $p-1$, le numérateur de B_n contiendra p^i; comme corollaire, on peut remarquer que, p étant un nombre premier quelconque, le numérateur de B_p contiendra toujours p. Quant aux nombres de la série pour la sécante qu'on peut nommer les nombres d'Euler qui le premier en a fait le calcul, et qui sont tous, comme on sait, des nombres entiers et positifs, et que je propose de dénoter par le symbole E, voici une propriété dont ils jouissent.

Désignons par p un nombre premier tel que $p-1$ ou plus généralement $(p-1)p^i$ soit un facteur de $2n$; alors, dans le cas où p est de la forme $4h+1$, p^{i+1} sera un facteur de E_n, mais dans le cas où p est de la forme $4h-1$, p^{i+1} sera un facteur de $2(-1)^{n-1}+E_n$. On comprend que E_n exprime le coefficient de $\frac{x^{2n}}{1.2\ldots 2n}$ dans le développement de sécante de x. Par parenthèse il sera bon de remarquer qu'en combinant les deux règles pour B_n et E_n on voit que le dénominateur de leur produit ne peut les contenir comme facteurs aucuns nombres premiers de la forme $4k+1$.

Euler a fait le calcul des E jusqu'à E_9, mais a donné une valeur erronée de cette dernière qui a été corrigée par M. Rothe, dans le *Journal de Crelle*, dans un Mémoire communiqué par M. Ohm*. Selon ma règle E_9+2 doit contenir les trois facteurs 3, 7, 19, ce qui s'accorde avec la valeur donnée par Rothe, mais non pas avec celle d'Euler. C'est à propos de ma nouvelle théorie des partitions des nombres que je me suis intéressé spécialement aux nombres de Bernoulli et d'Euler, qui tous les deux font une partie des développements qu'elle exige; en effet, on a besoin dans cette théorie de toutes les espèces de nombres dont la fonction génératrice est $\Sigma \frac{\rho^g}{e^t-\rho}$ (g étant un entier quelconque donné, et ρ une racine de l'unité d'un degré quelconque). Selon le degré de l'équation dont ρ est une racine primitive, on peut les nommer des nombres bernoulliens (ou si l'on veut sous-bernoulliens) d'un tel ou tel ordre. Jusqu'à présent on paraît n'avoir tenu compte que des nombres bernoulliens du premier et du second ordre (qui sont liés entre eux par le facteur exponentiel si bien connu) et de ceux du quatrième ordre auquel appartiennent en effet les nombres dits d'Euler. Mais ces nombres pour tous les ordres possèdent des propriétés arithmétiques très-dignes d'être étudiées; j'espère pouvoir y revenir et avoir l'honneur d'en faire le sujet d'une nouvelle communication à l'Académie.

[* Bd xx.]