38.

NOTE RELATIVE AUX COMMUNICATIONS FAITES DANS LES SÉANCES DES 28 JANVIER ET 4 FÉVRIER 1861.

(*Extrait d'une Lettre adressée à* M. Serret *par* M. Sylvester.)

[*Comptes Rendus de l'Académie des Sciences*, LII. (1861), pp. 307, 308.]

Dans la Note que j'ai eu l'honneur de présenter récemment à l'Académie et qui a été insérée au *Compte rendu* de la séance du 4 février dernier, j'ai fait connaître un théorème qui lie entre elles deux congruences, dont l'une se rapporte aux *indices* des nombres d'Euler et l'autre à ces nombres eux-mêmes; et, en même temps, j'ai avancé* qu'un théorème analogue doit avoir lieu pour les nombres de Bernoulli. Voici en quoi consiste ce théorème:

Soient p un nombre premier, n et n' deux nombres entiers dont les doubles $2n$, $2n'$ ne contiennent aucun des facteurs $p, p-1$, et soient congrus suivant le module $(p-1)\,p^i$ (i étant un entier quelconque positif ou nul); les nombres de Bernoulli B_n et $B_{n'}$ seront liés entre eux par la congruence

$$(-)^n \frac{B_n}{n} \equiv (-)^{n'} \frac{B_{n'}}{n'} \quad (\text{mod } p^{i+1}).$$

On doit remarquer que, d'après les conditions de l'énoncé, p ne peut être égal ni à 2, ni à 3.

Pour donner un exemple de ce théorème, prenons $n=7$, $n'=17$; les nombres $2n$ et $2n'$ seront congrus par rapport à $11-1$ et aussi par rapport à $(5-1)\,5$; d'ailleurs

$$\frac{B_7}{7} = \frac{1}{6}, \quad \frac{B_{17}}{17} = \frac{2\,577\,687\,858\,367}{17 \times 6};$$

par conséquent, on aura

$$\frac{B_7}{7} - \frac{B_{17}}{17} = -\frac{2\,577\,687\,858\,350}{102} \equiv 0 \quad (\text{mod } 11 \times 25),$$

ce que l'on peut vérifier immédiatement.

* Voir à la page [232] de ce volume.

Je profite de cette occasion pour présenter une remarque importante au sujet de la formule par laquelle j'ai exprimé [p. 230 above] le résidu de $\frac{r^{p-1}-1}{p}$ suivant le module p, dans le cas où l'on a $r=2$. Cette formule peut être remplacée avec avantage par la suivante :

$$\frac{2^{p-1}-1}{p} \equiv -\frac{\frac{1}{2}}{p-1}+\frac{\frac{1}{2}}{p-2}-\frac{\frac{1}{2}}{p-3}+\ldots \pmod{p},$$

qui est tout à fait semblable aux formules relatives au cas où r est un nombre premier impair, et qui n'exige pas, comme celle que j'avais trouvée d'abord, que l'on distingue les formes $4k+1$ et $4k-1$ du module premier p.

Pour ce qui concerne le cas où la base r du quotient de Fermat $\frac{r^{p-1}-1}{p}$ est un nombre composé, il n'y a aucune difficulté à exprimer le résidu de ce quotient suivant le module p, par des suites de fractions dont les dénominateurs sont les nombres inférieurs à p, et dont les numérateurs constituent des cycles exactement comme dans le cas où r est un nombre premier. Pour obtenir, en effet, les suites dont je viens de parler, il suffit de faire usage de la congruence évidente

$$\frac{(abc\ldots k)^{p-1}-1}{p} \equiv \frac{(a^{p-1}-1)+(b^{p-1}-1)+(c^{p-1}-1)+\ldots+(k^{p-1}-1)}{p} \pmod{p},$$

dans laquelle $a, b, c, \ldots, k$, désignent des entiers quelconques égaux ou inégaux. Au moyen de cette congruence, on ramène immédiatement, par de simples additions, le cas où r est un nombre composé au cas où cette base est un nombre premier.