

Sur les congruences du second degré et les nombres de Bernoulli.

Par

TAMARKINE et FRIEDMANN à St. Pétersbourg.

Prenons la congruence

$$(I) \quad x^2 \equiv q \pmod{p}$$

où q est un nombre entier, non congru à zéro suivant le module p , p un nombre premier impair. Supposons encore, qu'on ait:

$$\left(\frac{q}{p}\right) = 1,$$

c'est-à-dire que cette congruence soit résoluble en nombres entiers.

Dans le cas de $p = 4n - 1$ on sait que le couple des solutions de la congruence (I) sera:

$$x \equiv \pm q^{\frac{p+1}{4}} \pmod{p}.$$

Mais dans le cas de $p = 4n + 1$ nous ne connaissons aucune formule théorique pour la solution de la congruence (I).

Nous voulons donner ici une formule générale pour la solution de la congruence (I) dans les deux cas possibles: $p = 4n \mp 1$,

Théorème. Les deux solutions de la congruence (I) sont:

$$x \equiv \mp 2 \sum_{m=0}^{\frac{p-3}{2}} q^{\frac{p-1}{2}-m} \sum_{y=1}^{\frac{p-1}{2}} y^{2m+1}.$$

Démonstration. Prenons l'expression:

$$(1) \quad \sum_{y=1}^{\frac{p-1}{2}} y [1 - (y^2 - q)^{\frac{p-1}{2}}].$$

1) Si le nombre $y = y_1$ vérifie la congruence (1), le terme correspondant de la somme est congru à y_1 suivant le module p , car:

$$y_1 [1 - (y_1^2 - q)^{\frac{p-1}{2}}] \equiv y_1 \pmod{p}.$$

2) Dans le cas contraire, ce terme sera congru à zéro suivant le module p .

Or, entre les limites de la sommation (1 jusqu'à $\frac{p-1}{2}$) on ne peut rencontrer qu'un seul nombre y_1 , qui vérifie la congruence (I). Ainsi la somme (1) est congrue à y_1 suivant le module p , c'est-à-dire à la *racine**) de la congruence (I) qui est $< \frac{p}{2}$. L'autre solution sera évidemment congrue à $-y_1$.

Ainsi on peut écrire:

$$(II) \quad x \equiv \pm \sum_{y=1}^{\frac{p-1}{2}} y [1 - (y^2 - q)^{\frac{p-1}{2}}] \pmod{p}.$$

En transformant cette formule on peut la réduire à la suivante:

$$(III) \quad x \equiv \mp 2 \sum_{m=1}^{\frac{p-3}{2}} q^{\frac{p-1}{2}-m} \sum_{y=1}^{\frac{p-1}{2}} y^{2m+1} \pmod{p}. \quad \text{C. Q. F. D.}$$

La somme $\sum_{y=1}^{\frac{p-1}{2}} y^{2m+1}$ peut être effectuée à l'aide des fonctions de Bernoulli. En nous servant des notations de Markoff (voir «La théorie des différences», St.-Petersbourg 1899, t. II, pp. 23—33), nous écrivons:

$$\begin{aligned} \sum_{y=1}^{\frac{p-1}{2}} y^{2m+1} &\equiv (2m+1)! \varphi_{2m+2} \left(\frac{p+1}{2} \right) \equiv (2m+1)! \varphi_{2m+2} \left(\frac{1}{2} \right) \\ &\equiv \frac{(-1)^{m+1} B_{m+1}}{m+1} \cdot \frac{2^{2m+2} - 1}{2^{2m+2}} \pmod{p}. \end{aligned}$$

La dernière forme s'obtient en remplaçant $\varphi \left(\frac{1}{2} \right)$ par sa valeur.

Substituant cette valeur de la somme $\sum_{y=1}^{\frac{p-1}{2}} y^{2m+1}$ dans la formule (III) nous trouvons:

$$(IV) \quad x \equiv \mp 2 \sum_{m=0}^{\frac{p-3}{2}} q^{\frac{p-1}{2}-m} \cdot \frac{(-1)^{m+1} B_{m+1}}{m+1} \cdot \frac{2^{2m+2} - 1}{2^{2m+2}} \pmod{p}.$$

*) Nous appelons *racines* de la congruence celles des solutions positives qui sont $< p$.

Quand $m \leq \frac{p-5}{2}$, le nombre B_{m+1} ne contient pas le nombre p au dénominateur; mais quand $m = \frac{p-3}{2}$, on sait que:

$$\left(\frac{-1}{p}\right) B_{\frac{p-1}{2}} \cdot p \equiv 1 \pmod{p}.$$

Ainsi on peut écrire:

$$(V) \quad x \equiv \mp 2 \sum_{m=0}^{\frac{p-5}{2}} q^{\frac{p-1}{2}-m} \cdot \frac{(-1)^{m+1} B_{m+1}}{m+1} \cdot \frac{2^{2m+2}-1}{2^{2m+2}} \pm q \frac{2^{p-1}-1}{p} \pmod{p}.$$

La formule (V) donne le couple des solutions de la congruence (I).

A l'aide de la formule (V) on peut déduire de nombreuses formules pour les nombres de Bernoulli. Donnons-en les plus intéressantes.

Posons pour abrégé:

$$a_m = \frac{(-1)^{m+1} B_{m+1}}{m+1} \cdot \frac{2^{2m+2}-1}{2^{2m+2}} \quad \left(m \leq \frac{p-5}{2}\right),$$

$$a_{\frac{p-3}{2}} = -\frac{2^{p-1}-1}{p}.$$

Avec cette notation la formule (V) prendra la forme:

$$(VI) \quad x \equiv \mp 2 \sum_{m=0}^{\frac{p-3}{2}} a_m q^{\frac{p-1}{2}-m} \pmod{p}.$$

1) Posons $q \equiv 1 \pmod{p}$. Alors nous déduirons de la formule (VI):

$$1 \equiv -2 \sum_{m=0}^{\frac{p-3}{2}} a_m \equiv -2 \sum_{m=0}^{\frac{p-5}{2}} \frac{(-1)^{m+1} B_{m+1}}{m+1} \cdot \frac{2^{2m+2}-1}{2^{2m+2}} + \frac{2^{p-1}-1}{p} \pmod{p}.$$

2) Nous donnons une méthode générale pour obtenir des formules intéressantes sur les nombres de Bernoulli.

Pour cela, on écrira au lieu de la formule (VI) la formule suivante

$$(VII) \quad x \equiv -2 \sum_{m=0}^{\frac{p-3}{2}} a_m q^{\frac{p-1}{2}-m} \pmod{p}$$

où x représente maintenant la *racine* positive de la congruence (I), $< \frac{p}{2}$. En appelant β une racine primitive de la congruence

$$(2) \quad y^n \equiv 1 \pmod{p}$$

nous obtenons

$$(3) \quad (-1)^{\left[\frac{2\beta}{p}\right]} \beta \equiv -2 \sum_{m=0}^{\frac{p-3}{2}} a_m \beta^{p-1-2m} \pmod{p}.$$

Multiplions la congruence (3) par β^{2k} ($k < n$) et sommons les expressions obtenues pour toutes les racines de la congruence (2). Alors il viendra:

$$\sum_{\beta} (-1)^{\left[\frac{2\beta}{p}\right]} \beta^{2k+1} \equiv -2 \sum_{m=0}^{\frac{p-3}{2}} a_m \sum_{\beta} \beta^{p-1-2m+2k} \pmod{p}.$$

La somme $\sum_{\beta} \beta^{p-1-2m+2k} \equiv 0 \pmod{p}$, si n ne divise pas le nombre $p-1-2m-2k$. Dans le cas contraire, cette somme est congrue à n suivant le module p . On trouvera sans difficulté l'expression suivante:

$$(VIII) \quad \sum_{\beta} (-1)^{\left[\frac{2\beta}{p}\right]} \beta^{2k+1} \equiv -2n[a_k + a_{k+n} + \dots + a_{k+tn}],$$

où

$$k + tn \leq \frac{p-3}{2}, \quad k + (t+1)n > \frac{p-3}{2}.$$

St. Pétersbourg, 6 octobre 1905.
