Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 24 (1924-1925)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SOMMES DES PUISSANCES SEMBLABLES DES p—1 PREMIERS NOMBRES ENTIERS, p ÉTANT UN NOMBRE PREMIER

Autor: Lévy, A.

DOI: https://doi.org/10.5169/seals-515762

Dans l'exemple cité où p et q ont les valeurs (12), on peut prendre $h = 5$ et l'on aura

$$S = \frac{(2 \cdot 10^5 + 1)^{10}}{10^{50} - 10^{45}} =$$

$$= 0{,}06144\,17664\,33024\,46464\,54528\,57888\,58848\,59028\,59048\,59049 \; .$$

La probabilité pour que, sur dix épreuves, l'événement A arrive au moins 10–k fois (et B au plus k fois) s'obtient en divisant par 59049 le groupe de décimales de S commençant par la $(hk+1)^{\text{ième}}$ et terminée par la $(k+1)h^{\text{ième}}$ décimale. Ainsi, pour que A arrive au moins six fois (B au plus quatre fois), il y a la probabilité

$$Q_4 = \frac{46\,464}{59\,049} = 0{,}786872 \; ,$$

et pour que B arrive au plus dix fois (la certitude), il y a bien la probabilité

$$Q_{10} = \frac{59\,049}{59\,049} = 1 \; .$$

Mai 1925.

SOMMES DES PUISSANCES SEMBLABLES DES $p-1$ PREMIERS NOMBRES ENTIERS, p ÉTANT UN NOMBRE PREMIER

PAR

A. Lévy (Paris).

On sait que la congruence

$$x^{p-1} - 1 \equiv 0 \qquad \text{module } p \; , \qquad\qquad (p \text{ premier})$$

admet comme racines, 1, 2, ..., $p-1$. Les coefficients de cette congruence sont

$$a_1 \equiv 0 \; , \qquad a_2 \equiv 0 \; , \; \ldots \; , \; a_{p-2} \equiv 0 \; , \qquad a_{p-1} \equiv 1 \; ,$$

où la forme de la congruence générale est

$$x^{p-1} - a_1 x^{p-2} + a_2 x^{p-3} + \ldots + a_{p-1} \equiv 0 \; , \qquad \text{module } p.$$

Par suite, si l'on désigne par A_1 la somme des nombres $1+2+3+\dots(p-1)$, par A_k la somme des produits des nombres pris k à k, on a

$$A_k \equiv 0 \quad \text{module } p\,, \qquad A_{p-1}+1 \equiv 0\,, \quad \text{module } p\,.$$

On sait aussi que si l'on désigne par S_k la somme des puissances semblables

$$S_k^{p-1} = 1^k + 2^k + \dots + (p-1)^k\,,$$

on a

$$S_k \equiv 0\,, \qquad \text{mod. } p$$

pour $k = 1, 2, \dots, (p-2)$.

Théorème. — *Le numérateur de* S_{2i}^p *contient le facteur* $p(p+1)(2p+1)$ *et le numérateur de* S_{2i+1}^p *contient le facteur* $p^2(p+1)^2$.

Soit le polynome

$$\varphi_n(x) = (x+1)^n + (x+2)^n + \dots + (x+p)^n\,.$$

En développant

$$\varphi_n(x) = x^n + C_n^1 S_1^p x^{n-1} + C_n^2 S_2^p x^{n-2} + \dots + S_n^p\,.$$

Si n est impair

$$\varphi_n(-x) = -x^n + C_n^1 S_1^p x^{n-1} - C_n^2 S_2^p x^{n-2} + \dots + S_n^p\,.$$

Donc

$$\varphi_n(x) + \varphi_n(-x) = 2\left[S_n^p + C_n^2 S_{n-2}^p x^2 + C_n^4 S_{n-4}^p x^4 + \dots + C_n^{n-1} S_1^p x^{n-1}\right].$$

Faisons $x = 1$ dans cette formule, nous obtiendrons

$$\begin{aligned} &2^n + 3^n + \dots + (p+1)^n + 1^n + 2^n + \dots + (p-1)^n \\ &= 2(1^n + 2^n + \dots + p^n) + 2\left[C_n^2 S_{n-2}^p + C_n^4 S_{n-4}^p + \dots + C_n^{n-1} S_1^p\right]. \end{aligned}$$

En mettant $2S_1^p = p(p+1)$, cette formule s'écrit

$$\begin{aligned} &(p+1)^n - p^n - 1 - np(p+1) \\ &\qquad = 2\left[C_n^2 S_{n-2}^p + C_n^4 S_{n-4}^p + \dots + C_n^{n-3} S_3^p\right]. \qquad (1) \end{aligned}$$

Le polynome en p

$$(p+1)^n - p^n - 1 - np(p+1)$$

est divisible par $p^2(p+1)^2$, on peut vérifier en faisant $p=0$, $p+1=0$ dans ce polynome et sa dérivée par rapport à p.

Or $S_3^p = \frac{p^2(p+1)^2}{4}$. Mais on a

$$(p+1)^7 - p^7 - 1 - 7p(p+1) = 2C_7^2 S_5^p + 2C_7^2 S_3^p,$$

donc S_5^p contient $p^2(p+1)^2$ en facteur et la formule de récurrence trouvée prouve que ce résultat reste le même pour S_7^p, S_9^p, S_{11}^p, etc.

Supposons maintenant n pair. Alors

$$\varphi_n(x) + \varphi_n(-x) = 2\left[S_n^p + C_n^2 S_{n-2}^p x^2 + C_n^4 S_{n-4}^p x^4 + \dots + x^n\right]. \qquad (2)$$

Faisons $x=1$, après toutes les réductions, on aura

$$(p+1)^n - p^n - 2p - 1 = 2\left[C_n^2 S_{n-2}^p + C_n^4 S_{n-4}^p + \dots + C_n^{n-2} S_2^p\right],$$

Le polynome du premier membre est divisible par le facteur $p(p+1)(2p+1)$ et comme $S_2^p = \frac{p(p+1)(2p+1)}{6}$, S_4^p admettra le même facteur et de même S_6^p, S_8^p .... *Le théorème est vrai pour* $n = 2, 4, \dots, (p-3)$ *et non pour* $n = p-1$.

Corollaire. — En remplaçant p par $p-1$, on voit que le numérateur de S_{2i+1}^{n-1} est divisible par $(p-1)p(2p-1)$ et que le numérateur de S_{2i+1}^{p-1} contient le facteur $(p-1)^2 p^2$.

Si p est premier, S_{2i}^{p-1} est divisible par p, S_{2+i}^{p-1} est divisible par $(p-1)^2$.

De plus, si $2p-1$ est premier, S_{2i}^{p-1} est divisible par $2p-1$ et si $2p+1$ est premier, S_{2i}^p est divisible par $2p+1$.

Théorème. — Si l'on désigne par A_n^{p-1} le produit n à n des $(p-1)$ premiers nombres entiers, le nombre A_n^{p-1} est divisible par p. *Il l'est aussi par p^2 pour n impair supérieur à un.*

Je considére les formules

$$(x+1)(x+2)\dots(x+p-1)$$
$$= x^{p-1} + A_1^{p-1}x^{p-2} + \dots + A_{p-2}^{p-1}x + A_{p-1}^{p-1}, \qquad (1)$$

$$(x-1)(x-2)\dots(x-p+1)$$
$$= x^{p-1} - A_1^{p-1}x^{p-2} + A_2^{p-1}x^{p-3} - \dots - A_{p-2}^{p-1}x + A_{p-1}^{p-1} \qquad (2)$$

En faisant la différence et en donnant à n la valeur 1, on a

$$p\,! = 2\left[A_1^{p-1} + A_3^{p-1} + \dots + A_{p-2}^{p-1}\right] .$$

En retranchant A_1^{p-1}, on a

$$p\,! - p(p-1) = 2\left[A_3^{p-1} + A_5^{p-1} + \dots + A_{p-2}^{p-1}\right] .$$

ou encore

$$p[(p-1)\,! + 1 - p] = 2\left[A_3^{p-1} + A_5^{p-1} + \dots + A_{p-2}^{p-1}\right] .$$

Le premier membre se divise par p^2, puisque

$$(p-1)\,! + 1 \equiv 0 . \qquad \text{module } p$$

(théorème de Wilson).

En faisant la différence de (1) et de (2) pour $x = 2$, on trouve

$$3.4 \dots p(p+1) = 2\left[2^{p-2} A_1^{p-1} + 2^{p-4} A_3^{p-1} + \dots + 2A_{p-2}^{p-1}\right] ,$$

en retranchant $A_1^{p-2} \times 2^{p-1}$ des deux membres, on a

$$\begin{aligned} 3.4 \dots p(p+1) &- 2^{p-1} p(p-1) \\ &= 2^2\left[2^{p-5} A_3^{p-1} + 2^{p-7} A_5^{p-1} + \dots + A_{p-2}^{p-1}\right] , \end{aligned}$$

ou encore

$$\begin{aligned} p[2.3 \dots (p-1)(p+1) &- 2^{p-1}(p-1)] \\ &= 4\left[2^{p-5} A_3^{p-1} + 2^{p-7} A_5^{p-1} + \dots + A_{p-2}^{p-2}\right] . \end{aligned}$$

En vertu des théorèmes de Wilson et de Fermat [1], le second facteur du premier membre est de la forme

$$(kp-1)(p+1) - (mp+1)(p-1) ,$$

nombre qui contient p en facteur. Le premier membre est donc divisible par p^2. En faisant les mêmes opérations sur les formules (1), (2) mais pour $x = 3, 4, \dots, (p-1)$, on arrive à remarquer que la congruence

$$A_3^{p-1} x^{p-4} + A_5^{p-1} x^{p-6} + \dots + A_{p-2}^{p-1} x \equiv 0 \qquad \text{mod. } p^2$$

[1] Les calculs faits au moment de ces remarques peuvent, comme le lecteur l'aura constaté, donner une démonstration du théorème de Wilson, et aussi une démonstration du théorème de Fermat.

admet plus de $p-1$ racines, ce qui exige

$$A_3^{p-1} \equiv 0 \ , \qquad \text{mod. } p^2$$

$$A_5^{p-1} \equiv 0 \ , \qquad \text{mod. } p^2$$

$$\vdots$$

$$A_{p-2}^{p-1} \equiv 0 \ . \qquad \text{mod. } p^2$$

Corollaire. — L'expression

$$(p+1)(p+2)\ldots(2p-1) - 1.2\ldots(p-1)$$

est divisible par p^3 et par suite aussi

$$\frac{(p+1)(p+2)\ldots(2p-1)}{1.2\ldots(p-1)} - 1 \ .$$

En effet

$$(p+1)(p+2)\ldots(p+p-1) = p^{p-1} + A_1^{p-1}p^{p-2} + \ldots + A_{p-1}^{p-1}$$

$$A_{p-1}^{p-1} = (p-1)(p-2)\ldots[p-(p-1)] = p^{p-1} - A_1^{p-1}p^{p-2} + \ldots + A_{p-1}^{p-1} \ ,$$

donc

$$(p+1)(p+2)\ldots(2p-1) - (p-1)! \\ = 2\left[p^{p-2}A_1^{p-1} + p^{p-4}A_3^{p-1} + \ldots + pA_{p-2}^{p-1}\right] .$$

D'après ce qui précède, le second membre est divisible par p^3. Il en sera de même pour l'expression donnée.