C. R. Acad. Sci. Paris, Ser. I 348 (2010) 479–482

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Théorie des nombres

Sur l'équation $x^{p^{m-1}} + y^{p^{m-1}} + z^{p^{m-1}} \equiv 0 \bmod p^m$ ☆

On the equation $x^{p^{m-1}} + y^{p^{m-1}} + z^{p^{m-1}} \equiv 0 \bmod p^m$

François Apéry

F.S.T., 68093 Mulhouse cedex, France

I N F O A R T I C L E

Historique de l'article :
Reçu le 19 septembre 2009
Accepté après révision le 2 mars 2010
Disponible sur Internet le 20 mars 2010

Présenté par Jean-Pierre Serre

R É S U M É

On démontre la formule $\sum_{m\geqslant 1} S_m(p) = (p-1)\operatorname{val}_p W_{p-1}$, où W_{p-1} est le nombre de Wendt d'ordre $p-1$, et $S_m(p)$ est le nombre de classes de solutions non triviales de $x^{p^{m-1}} + y^{p^{m-1}} + z^{p^{m-1}} \equiv 0 \bmod p^m$. Dans le cas $p \equiv 1 \bmod 6$, la sommation est infinie, mais on obtient une formule analogue avec une somme finie en considérant les classes de solutions non triviales et non cycliques et le nombre de Wendt réduit.

A B S T R A C T

The formula $\sum_{m\geqslant 1} S_m(p) = (p-1)\operatorname{val}_p W_{p-1}$ is proved, where W_{p-1} is the Wendt number of order $p-1$, and $S_m(p)$ denotes the number of nontrivial solution classes of $x^{p^{m-1}} + y^{p^{m-1}} + z^{p^{m-1}} \equiv 0 \bmod p^m$. In the case $p \equiv 1 \bmod 6$, the sum is infinite, however, we obtain a similar formula with a finite sum by considering the nontrivial and noncyclic solution classes as well as the reduced Wendt number.

1. Introduction

Deux éléments de $\mathbb{Z}^3$ congrus modulo $(p\mathbb{Z})^3$ seront dit équivalents. Si $(x', y', z') \in \mathbb{Z}^3$ est équivalent à une solution de la congruence de Fermat

$$x^{p^{m-1}} + y^{p^{m-1}} + z^{p^{m-1}} \equiv 0 \bmod p^m, \tag{1}$$

où p est un nombre premier et $m \geqslant 1$, alors, (x', y', z') est solution de (1). De même, tout triplet équivalent à une solution non triviale (x, y, z), autrement dit, telle que $xyz \not\equiv 0 \bmod p$, est une solution non triviale. Soit $\mathcal{S}_m$ l'ensemble des solutions non triviales de (1), et $\Sigma_m := \mathcal{S}_m/\sim$ celui des classes d'équivalence de solutions non triviales, **considéré comme une partie de** $(\mathbb{F}_p^*)^3$. On pose $S_m(p) := \operatorname{card} \Sigma_m$. C'est une fonction décroissante de m. On a $S_1(p) = (p-1)(p-2)$. Par ailleurs, on utilise les nombres (appelés déterminants de Wendt (voir par ex. [1], p. 219)) définis pour $n \geqslant 1$ par

$$W_n := \det\left(\binom{n}{|i-j|}\right)_{1\leqslant i,j\leqslant n} = \operatorname{Res}_{n,n}\bigl(X^n - 1, (X+1)^n - 1\bigr) \in \mathbb{Z}.$$

On désigne par val_p la valuation p-adique. Le but de cette Note est de prouver les deux théorèmes suivants :

☆ Cette Note doit beaucoup d'améliorations à J.-P. Jouanolou, Y. Hellegouarch et J.-P. Serre.

Adresse e-mail : francois.apery@uha.fr.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2010.03.005

Théorème 1.1. *Si p est un nombre premier, on a l'égalité*

$$\sum_{m\geqslant 1} S_m(p) = (p-1)\operatorname{val}_p W_{p-1}. \tag{2}$$

Sachant que W_n s'annule, autrement dit $\operatorname{val}_p W_n = +\infty$, si et seulement si $n \equiv 0 \bmod 6$ (voir par ex. [6], p. 127), on en déduit que si $p \not\equiv 1 \bmod 6$, alors $\operatorname{val}_p W_{p-1}$ est fini et $S_m(p)$ s'annule donc pour m suffisamment grand. Dans le cas $p \equiv 1 \bmod 6$, on introduit le **nombre de Wendt réduit** W'_q défini, lorsque $n = 6q$, par le résultant

$$W'_q := \operatorname{Res}_{n-2,n}\left(\frac{X^n-1}{X^2+X+1}, (X+1)^n - 1\right) \in \mathbb{Z}.$$

La notation $\operatorname{Res}_{m,n}$ désigne le résultant en degrés m et n [3]. On appelle **solution cyclique** de (1), toute solution (nécessairement non triviale) s'écrivant sous la forme $b(1, a, a^2)$ avec $ab \neq 0$ et $(a, b) \in \mathbb{Z}^2$. On désigne par $\mathcal{S}'_m$ l'ensemble des classes de solutions non triviales et non cycliques, et on pose $S'_m(p) := \operatorname{card} \mathcal{S}'_m$. Lorsque $p \equiv 1 \bmod 6$, on a $S_m(p) = S'_m(p) + 2(p-1)$.

Théorème 1.2. *Si $p = 1 + 6q$ est un nombre premier, on a l'égalité*

$$\sum_{m\geqslant 1} S'_m(p) = 6q \operatorname{val}_p W'_q. \tag{3}$$

Sur $\mathbb{C}$, W_n se décompose sous la forme $\prod_{\zeta^n=1}((\zeta+1)^n - 1)$ (voir par ex. [1], prop. 9, p. 22 appliquée à la formule de l'exer. 56.1, p. 220), or, si $(\zeta+1)^n - 1 = 0$, alors $\zeta + 1$ et ζ sont deux racines $n^{\text{ème}}$ de l'unité, donc $\zeta = j$ ou j^2. Il s'ensuit que, dans le cas où $n = 6q$, le nombre de Wendt réduit W'_q, qui s'écrit $\prod_{\zeta^n=1,\zeta\neq j,j^2}((\zeta+1)^n - 1)$, ne s'annule pas. On en déduit que $S'_m(p)$ s'annule pour m suffisamment grand.

Le cas $p = 2$ étant évident, on supposera dorénavant que p est un nombre premier impair.

2. Lemmes préparatoires

On désigne par $\mathbb{Z}_p$ l'anneau des entiers p-adiques et par $\mathbb{Z}_p \xrightarrow{\alpha_m} \mathbb{Z}/p^m\mathbb{Z}$ la projection canonique. On a

$$\ker \alpha_m = \{\omega \in \mathbb{Z}_p\colon \operatorname{val}_p \omega \geqslant m\} = p^m\mathbb{Z}_p. \tag{4}$$

Soit $s_1 : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_p$ l'unique application (qui se trouve être multiplicative) telle que

$$\overline{x^{p^{m-1}}} = \alpha_m \circ s_1(\bar{x}), \tag{5}$$

où $\bar{x}$ désigne la classe mod p de $x \in \mathbb{Z}$ et $\overline{x^{p^{m-1}}}$ la classe mod p^m. On pose

$$\Sigma'_m := \left\{(\bar{x}, \bar{y}, \bar{z}) \in \left(\mathbb{F}_p^*\right)^3\colon \delta_2(\bar{x}, \bar{y}, \bar{z}) \geqslant m\right\},$$

où $\delta_2(\bar{x}, \bar{y}, \bar{z}) := \operatorname{val}_p(s_1(\bar{x}) + s_1(\bar{y}) + s_1(\bar{z}))$ (on emprunte cette notation à [5]). La relation (5) jointe à (4) prouve l'énoncé suivant :

Lemme 2.1. *L'application $(x, y, z) \mapsto (\bar{x}, \bar{y}, \bar{z})$ définit une application de $\mathcal{S}_m$ sur Σ'_m qui se factorise à travers Σ_m et induit une bijection de Σ_m sur Σ'_m.*

Le groupe multiplicatif $\mathbb{F}_p^*$ opère par multiplication terme à terme sur Σ'_m. L'opération est simple, donc chaque orbite a $p-1$ éléments. Notant $\Sigma'_m/\sim$ l'ensemble des orbites, on a facilement :

Lemme 2.2. *L'application $\varphi : (\bar{x}, \bar{y}, \bar{z}) \mapsto (\frac{\bar{x}}{\bar{z}}, \frac{\bar{y}}{\bar{z}})$ définie sur Σ'_m, se factorise à travers $\Sigma'_m/\sim$ et induit une bijection de $\Sigma'_m/\sim$ sur $T_m := \{(\bar{x}, \bar{y}) \in (\mathbb{F}_p^*)^2\colon \delta_2(1, \bar{x}, \bar{y}) \geqslant m\}$. En particulier $(p-1)\operatorname{card} T_m = S_m(p)$.*

Si $(\bar{x}, \bar{y}) \in T_m$, alors $(\bar{x}, \bar{y}, 1) \in \Sigma'_m \subseteq \Sigma'_1$, donc $s_1(\bar{x}) + s_1(\bar{y}) + s_1(1) \in \ker \alpha_1$, autrement dit

$$1 + \bar{x} + \bar{y} = \alpha_1\big(s_1(\bar{x}) + s_1(\bar{y}) + s_1(1)\big) = 0,$$

de sorte que l'application $\bar{x} \mapsto (\bar{x}, -1-\bar{x})$ définit une bijection de $T'_m := \{\bar{x} \in \mathbb{F}_p^*\colon \delta_2(1, \bar{x}, -1-\bar{x}) \geqslant m\}$ sur T_m. En particulier, comme $\delta_2(1, -1, 0) = \operatorname{val}_p(2) = 0$, on a $-1 \notin T'_m$. Notons également que si $\bar{x} \in T'_m$, alors $-1-\bar{x} \in T'_m$. On a $\operatorname{card} T'_m = \operatorname{card} T_m = S_m(p)/(p-1)$. On désigne par $G(p^m)$ le groupe des unités de $\mathbb{Z}/p^m\mathbb{Z}$, et par $\mu_{p-1}(p^m)$ le sous-groupe des racines $(p-1)$-èmes de l'unité. En particulier, $G(p) = \mu_{p-1}(p) = \mathbb{F}_p^*$, et plus généralement $\mu_{p-1}(p^m) \simeq \mathbb{F}_p^*$. On a

$$G\big(p^m\big) \simeq \mu_{p-1}\big(p^m\big) \times G_1\big(p^m\big) \simeq \mathbb{F}_p^* \times G_1\big(p^m\big),$$

où $G_1(p^m) := 1 + p\mathbb{Z}/p^m\mathbb{Z}$. On note $\alpha_{1,m}$ le morphisme d'anneaux canonique de $\mathbb{Z}/p^m\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z}$ et on pose $s_{1,m} = \alpha_m \circ s_1$. On a $\alpha_{1,m} \circ s_{1,m} = \mathrm{id}_{\mathbb{F}_p}$.

Lemme 2.3. *$s_{1,m}(T'_m) = \mathcal{F}_m := \{\bar{x} \in \mu_{p-1}(p^m)\colon 1 + \bar{x} \in \mu_{p-1}(p^m)\}$, et* $\operatorname{card} \mathcal{F}_m = S_m(p)/(p-1)$.

Démonstration. On a $\operatorname{card} s_{1,m}(\mathbb{F}_p^*) = p - 1$, or $s_{1,m}$ est multiplicative (en particulier $s_{1,m}(1) = 1$), donc

$$s_{1,m}\big(\mathbb{F}_p^*\big) \subseteq G\big(p^m\big) \simeq \mu_{p-1}\big(p^m\big) \times G_1\big(p^m\big).$$

Or $\operatorname{card} \mu_{p-1}(p^m) = p - 1$ et $\operatorname{card} G_1(p^m) = p^{m-1}$, donc la projection de $s_{1,m}(\mathbb{F}_p^*)$ sur $G_1(p^m)$ est réduite à l'élément neutre, et $s_{1,m}(\mathbb{F}_p^*) = \mu_{p-1}(p^m)$. Si $\bar{x} \in T'_m$, alors $1 + s_1(\bar{x}) + s_1(-1-\bar{x}) \in \ker \alpha_m$, donc

$$1 + s_{1,m}(\bar{x}) + s_{1,m}(-1-\bar{x}) = \alpha_m\big(1 + s_1(\bar{x}) + s_1(-1-\bar{x})\big) = 0. \tag{6}$$

Puisque $-1 - \bar{x} \in T'_m$, on a $s_{1,m}(-1-\bar{x}) \in \mu_{p-1}(p^m)$, et, comme $p-1$ est pair, $1 + s_{1,m}(\bar{x}) = -s_{1,m}(-1-\bar{x}) \in \mu_{p-1}(p^m)$. Ceci prouve que $s_{1,m}(\bar{x}) \in \mathcal{F}_m$, donc que $s_{1,m}(T'_m) \subseteq \mathcal{F}_m$.

Inversement, si $\bar{x} \in \mathcal{F}_m$, $\bar{x}$ et $1 + \bar{x} \in \mu_{p-1}(p^m)$, et il existe $\bar{a}, \bar{b} \in \mathbb{F}_p^*$ tel que $\bar{x} = s_{1,m}(\bar{a})$ et $-1 - \bar{x} = s_{1,m}(\bar{b})$, de sorte que $1 + s_{1,m}(\bar{a}) + s_{1,m}(\bar{b}) = 0$. En appliquant $\alpha_{1,m}$ qui est additive, on en déduit que $1 + \bar{a} + \bar{b} = 0$. Par ailleurs, comme pour (6), on a $1 + s_1(\bar{a}) + s_1(-1-\bar{a}) = 1 + s_1(\bar{a}) + s_1(\bar{b}) \in \ker \alpha_m$, donc $\delta_2(1, \bar{a}, -1-\bar{a}) \geqslant m$, et par suite $\bar{a} \in T'_m$ et $\bar{x} \in s_{1,m}(T'_m)$, ce qui prouve l'inclusion $\mathcal{M}_m \subseteq s_{1,m}(T'_m)$. Le calcul du cardinal de $\mathcal{F}_m$ résulte de l'injectivité de $s_{1,m}$. □

Désignant par $\mu_{p-1}(p^\infty)$ le groupe des racines $(p-1)$-èmes de l'unité de $\mathbb{Z}_p$, l'application α_m se restreint à un isomorphisme de $\mu_{p-1}(p^\infty)$ sur $\mu_{p-1}(p^m)$.

Lemme 2.4. *Soit $m \geqslant 1$ et $\zeta \in \mu_{p-1}(p^\infty)$. Posant $\nu(\zeta) := (\zeta+1)^{p-1} - 1$, on a $\operatorname{val}_p \nu(\zeta) \geqslant m$ si et seulement si $\alpha_m(\zeta) \in \mathcal{F}_m$. En particulier, on a* $\operatorname{card}\{\zeta \in \mu_{p-1}(p^\infty)\colon \operatorname{val}_p \nu(\zeta) \geqslant m\} = S_m(p)/(p-1)$.

Démonstration. L'expression du cardinal résulte de la première partie de l'énoncé, et, puisque α_m se restreint à une bijection de $\alpha_m^{-1}(\mathcal{F}_m) \subseteq \mu_{p-1}(p^\infty)$ sur $\mathcal{F}_m \subseteq \mu_{p-1}(p^m)$, du Lemme 2.3. On démontre maintenant l'équivalence. Soit $\zeta \in \mu_{p-1}(p^\infty)$. Si $\operatorname{val}_p \nu(\zeta) \geqslant m$, on a $\alpha_m(\mu_{p-1}(p^\infty)) = \mu_{p-1}(p^m)$, donc $\alpha_m(\zeta) \in \mu_{p-1}(p^m)$. De plus $\nu(\zeta) \in \ker \alpha_m$, donc $\alpha_m(\zeta) + 1 \in \mu_{p-1}(p^m)$ et par suite, $\alpha_m(\zeta) \in \mathcal{F}_m$. Réciproquement, si $\alpha_m(\zeta) \in \mathcal{F}_m$, alors, $\alpha_m(\zeta) + 1 \in \mu_{p-1}(p^m) = \alpha_m(\mu_{p-1}(p^\infty))$, donc, il existe $\omega \in \mu_{p-1}(p^\infty)$ tel que $\alpha_m(\omega) = \alpha_m(\zeta) + 1$. On en déduit que $\zeta + 1 - \omega \in \ker \alpha_m = p^m\mathbb{Z}_p$, d'où [2, ch. IX, §1, lemme 1, p. 2] $(\zeta+1)^{p-1} \equiv \omega^{p-1} = 1 \bmod p^m\mathbb{Z}_p$, autrement dit $\operatorname{val}_p \nu(\zeta) \geqslant m$. □

3. Démonstration des Théorèmes 1.1 et 1.2

On a supposé $p \geqslant 3$. On décompose W_{p-1} dans $\mathbb{Z}_p$ sous la forme suivante (voir [1], p. 220) :

$$W_{p-1} = \prod_{\zeta \in \mu_{p-1}(p^\infty)} \nu(\zeta) = - \prod_{\zeta \in \mu_{p-1}(p^\infty) \setminus \{-1\}} \nu(\zeta), \tag{7}$$

où $\nu(\zeta) = (\zeta+1)^{p-1} - 1$. Sachant que $\operatorname{val}_p(\omega^{p-1} - 1) \geqslant 1$ pour tout $\omega \in \mathbb{Z}_p^*$, on en déduit

$$\operatorname{val}_p W_{p-1} = \sum_{\zeta \in \mu_{p-1}(p^\infty) \setminus \{-1\}} \operatorname{val}_p \nu(\zeta) = \sum_{m \geqslant 1} \operatorname{card}\big\{\zeta \in \mu_{p-1}\big(p^\infty\big)\colon \operatorname{val}_p \nu(\zeta) \geqslant m\big\}. \tag{8}$$

Le Lemme 2.4 conduit à la formule (2) du Théorème 1.1. On se place maintenant dans le cas où $p = 1 + 6q$ est un nombre premier. L'anneau $\mathbb{Z}_p$ admet deux racines primitives cubiques que nous désignerons, comme dans $\mathbb{C}$, par j et j^2. La décomposition de W'_q dans $\mathbb{Z}_p$, donne $\prod_{\zeta \in \mu_{p-1}(p^\infty), \zeta \neq j, j^2} \nu(\zeta)$. Si $b(1, a, a^2)$ avec $ab \neq 0$ et $(a, b) \in \mathbb{Z}^2$ est une solution cyclique de (1), on a $1 + \bar{a} + \bar{a}^2 = 0$ dans $\mathbb{F}_p$, donc, appliquant l'isomorphisme, noté par abus α_1^{-1}, de $\mu_{p-1}(p) = \mathbb{F}_p^*$ sur $\mu_{p-1}(p^\infty)$ et posant $\omega = \alpha_1^{-1}(\bar{a})$, on a $1 + \omega + \omega^2 = 0$ dans $\mathbb{Z}_p$, de sorte que ω est une racine primitive cubique de l'unité, en particulier $p \equiv 1 \bmod 6$. Il en résulte que, comme dans le Lemme 2.2, le groupe $\mathbb{F}_p^*$ opère sur $\mu_{p-1}(p^\infty) \setminus \{j, j^2\}$, et que

$$(p-1)\operatorname{card}\big\{\zeta \in \mu_{p-1}\big(p^\infty\big) \setminus \big\{\alpha_m(j), \alpha_m\big(j^2\big)\big\}\colon \operatorname{val}_p \nu(\zeta) \geqslant m\big\} = S_m(p) - 2(p-1).$$

La démonstration du Théorème 1.1 s'applique, mutatis mutandis, pour conduire à la formule (3) du Théorème 1.2. □

Remarque 3.1. D'après [4], il existe une constante A telle que pour tout $p \equiv -1 \bmod 6$,

$$\left|\ln(-W_{p-1}) - (p-1)^2\lambda\right| \leqslant \frac{A}{p-1},$$

où $\lambda = 0{,}323066\ldots$, par suite, d'après la formule (2), si p est un nombre premier $\not\equiv 1 \bmod 6$ suffisamment grand, sachant que $S_1(p) = (p-1)(p-2)$, on a

$$\sum_{m\geqslant 2} S_m(p) \leqslant (p-1)^2\left((p-1)\frac{\lambda}{\ln p} - 1\right) + p - 1.$$

Si p est un nombre premier $\equiv -1 \bmod 6$, il résulte d'un calcul de F. Recher ([5] et communic. privée, 2009) que $S_3(p) = 0$ pour $p \leqslant 104\,659$; aucune valeur de $p \equiv -1 \bmod 6$ n'annulant pas S_3 n'est connue.

Références

[1] F. Apéry, J.-P. Jouanolou, Élimination, le cas d'une variable, Hermann, Paris, 2006.
[2] N. Bourbaki, Éléments de mathématique ; Algèbre commutative, Masson, Paris, 1983 (ch. 8–9).
[3] N. Bourbaki, Éléments de mathématique ; Algèbre, Masson, Paris, 1981 (ch. 4, §6, n° 6).
[4] D.W. Boyd, The asymptotic behaviour of the binomial circulant determinant, J. Math. Anal. Appl. 86 (1982) 30–38.
[5] Y. Hellegouarch, F. Recher, Défaut d'additivité des chiffres de Teichmüller, C. R. Acad. Sci. Paris Sér. I 318 (1994) 401–406.
[6] P. Ribenboim, Fermat's Last Theorem for Amateurs, Springer, New York, 1999.