BULLETIN DE LA S. M. F.

P. LE LIDEC

Nouvelle forme des congruences de Kummer-Mirimanoff pour le premier cas du théorème de Fermat

Bulletin de la S. M. F., tome 97 (1969), p. 321-328

<http://www.numdam.org/item?id=BSMF_1969__97__321_0>

Bull. Soc. math. France,
97, 1969, p. 321 à 328.

NOUVELLE FORME DES CONGRUENCES DE KUMMER-MIRIMANOFF POUR LE PREMIER CAS DU THÉORÈME DE FERMAT

PAR

PAUL LE LIDEC (*).

1. — Soient p un nombre premier impair, et (a, b, c) une solution de l'équation de Fermat

$$x^p + y^p + z^p = 0 \tag{F}$$

telle que $abc \not\equiv 0 \pmod p$. MIRIMANOFF a déduit des congruences de Kummer les congruences suivantes :

$$f_i(t) f_{p-i}(t) \equiv 0 \pmod p, \tag{M}$$

$$i = 3, 5, \ldots, (p-2) \quad (1), \qquad t \equiv -\frac{b}{a} \pmod p,$$

auxquelles il faut ajouter la congruence

$$f_{p-1}(t) \equiv 0 \pmod p$$

qui n'est autre que le développement de $\dfrac{(t+1)^p - t^p - 1}{p} \equiv 0 \pmod p$.)

Le développement de $f_i(x)$ est le suivant :

$$f_i(x) = x^{p-1} + 2^{i-1}x^{p-2} + 3^{i-1}x^{p-3} + \ldots + (p-2)^{i-1}x^2 + (p-1)^{i-1},$$

c'est-à-dire

$$f_i(x) = \sum_{1=1}^{p-1} s^{i-1} x^{p-s}.$$

(*) *Thèse Univ.*, Fac. Sc. Paris, 1967, 2e partie (la première était un aperçu historique).

(1) Si l'on prend tous les $i = 2, 3, 4, \ldots, (p-2)$, on obtient les mêmes congruences, chacune répétée 2 fois, car $f_{p-i}(x) f_{p-(p-i)}(x) = f_i(x \mid f_{p-i}(x)$.

Le présent mémoire a pour but de déduire des congruences (M) d'autres congruences équivalentes de forme remarquable et qui semblent permettre l'application de méthodes combinatoires susceptibles d'aboutir à la démonstration du premier cas du théorème de Fermat.

Les calculs qui suivent sont des calculs de polynômes dans le corps Ω_p de p éléments. Sauf au moment de la conclusion, nous n'écrirons aucune congruence (mod p), les polynômes considérés étant supposés appartenir à $\Omega_p(x)$. Pour les besoins de la cause, nous munirons Ω_p de certaines autres structures, et adopterons provisoirement certains abus d'écriture.

1° Ω_p sera considéré de la manière habituelle comme un Z-module, où Z est l'anneau des entiers rationnels.

2° Quand nous exprimerons un entier rationnel n, ce signe, par abus d'écriture, signifiera le produit

$$n.1 = 1 + 1 + \ldots + 1 \ (n \text{ fois}) \text{ par } n \text{ de l'unité } 1 \text{ de } \Omega_p$$

alors que, dans de rares cas où nous en aurons besoin, l'entier rationnel sera noté n^*.

3° Ω_p étant considéré comme l'anneau quotient $\frac{Z}{(p)}$ de Z par son idéal (p), n désignera également la classe (mod p) de l'entier qu'il note normalement, ce second abus d'écriture n'entrant pas en conflit avec le premier.

4° Ω_p sera considéré comme totalement ordonné par l'ordre des plus petits restes non négatifs de ses éléments, considérés comme classes (mod p) dans l'anneau Z.

2. — On a visiblement la formule de récurrence

$$f_{i+1}(x) = -xf'_i(x),$$

où $f'(x)$ désigne la dérivée de $f(x)$.

D'autre part, si $1 \leq i < p$,

$$f_i(1) = \sum_{s=1}^{p-1} s^{i-1} = \sum_{s \in \Omega_p} s^{i-1} = 0,$$

tandis que

$$f_p(1) = \sum_{s=1}^{p-1} s^{p-1} = p - 1 \not\equiv 0.$$

Par suite, si $2 \leq i \leq p-1$ et si $f_{i+1}(x)$ est d'ordre J par rapport à $(x-1)$ dans $\Omega_p(x)$, $f_i(x)$ est d'ordre $j+1$. Il en résulte que l'ordre de $f_i(x)$ en $(x-1)$ dans $\Omega_p(x)$ est $p-i$.

Posons

$$g_i(x) = \frac{f_i(x)}{(x-1)^{p-i}}.$$

3. — Calculons d'abord $g_{p-1}(x)$ et, pour simplifier l'écriture, notons $\bar{q}$ l'inverse dans Ω d'un $q \in \Omega$ non nul. On a

$$g_{p-1}(x) = A_1^{(p-2)} x^{p-2} + A_2^{(p-2)} x^{p-3} + \ldots + A_{p-2}^{(p-2)} x,$$

avec

$$\begin{aligned} A_1^{(p-2)} &= \bar{1}, \\ A_2^{(p-2)} &= \bar{2} + \bar{1}, \\ &\ldots\ldots\ldots\ldots, \\ A_q^{(p-2)} &= \bar{q} + (\overline{q+1}) + \ldots + 1. \end{aligned}$$

On a donc

$$\begin{aligned} g_{p-1}(x) = x^{p-2} &+ (\bar{2} + \bar{1}) x^{p-3} + (\bar{3} + \bar{2} + \bar{1}) x^{p-4} + \ldots \\ &+ [(\overline{p-2}) + (\overline{p-3}) + \ldots + 1] x, \end{aligned}$$

d'où

$$g_{p-1}(x) = \sum_{s=1}^{p-2} \left(\sum_{q=1}^{s} \bar{q} \right) x^{p-1-s}.$$

4. — Calculons maintenant, pour $i = 2, 3, \ldots, (p-2)$, l'expression

$$g_i(x)\, g_{p-i}(x),$$

$$g_i(x)\, g_{p-i}(x) = \frac{f_i(x)}{(x-1)^{p-i}} \frac{f_{p-i}(x)}{(x-1)^i} = \frac{f_i(x)\, f_{p-i}(x)}{(x-1)^p} = \frac{f_i(x)\, f_{p-i}(x)}{x^p - 1}$$

On a $q^{(p-i)-1} = q^{p-1}\, q^{-i} = \bar{q}^i$,

$$(x^p - 1)\, g_i(x)\, g_{p-i}(x) = f_i(x)\, f_{p-i}(x) = \left(\sum_{q=1}^{p-1} q^{i-1} x^{p-q} \right) \left(\sum_{q'=1}^{p-1} \bar{q}'^i x^{p-q'} \right)$$

ou encore

$$\sum_{s=2}^{2p-2} \left(\sum_{q+q'=s} q^{i-1} \bar{q}'^i \right) x^{2p-s},$$

ce qui donne

$$g_i(x)\, g_{p-i}(x) = \sum_{s=2}^{p-2} \left(\sum_{q=1}^{s-1} \bar{q}^i (s-q)^{i-1} \right) x^{p-s}.$$

Ce produit est explicité comme suit.

Par exemple, si s = $p-3$, le coefficient du terme en $x^{p-(p-3)} = x^3$ est

$$\sum_{q=1}^{p-4} \bar{q}^i (p-3-q)^{i-1}.$$

n étant un entier quelconque tel que $1 \leq n \leq p-2$, posons

$$Q_n(x) = \sum_{s=2}^{p-2} u_s x^{p-s} = \sum_{i=2}^{p-2} n^i g_i(x)\, g_{p-i}(x),$$

u_s a donc pour valeur

$$\sum_{i=2}^{p-2} n^i \sum_{q=1}^{s-1} \bar{q}^i (s-q)^{i-1} = \sum_{q=1}^{s-1} \left(\sum_{i=2}^{p-2} n^i \bar{q}^i (s-q)^{i-1} \right) = \sum_{q=1}^{s-1} r_{s,q},$$

avec

$$r_{s,q} = \frac{1}{s-q} \left[\frac{[n\bar{q}(s-q)]^{p-1} - 1}{n\bar{q}(s-q) - 1} - n\bar{q}(s-q) - 1 \right].$$

Or, $n\bar{q}(s-q)^{p-1} - 1 = 0$, donc :

$$\underline{\text{si } n\bar{q}(s-q) \neq 1}, \quad r_{s,q} = \frac{-1}{s-q}[n\bar{q}(s-q)+1] = -[(\overline{s-q}) + n\bar{q}];$$

$$\underline{\text{si } n\bar{q}(1-q) = 1}, \quad r_{s,q} = (p-3)\frac{1}{s-q} = -\frac{3}{s-q}$$
$$= -[(\overline{s-q}) + n\bar{q} + n\bar{q}].$$

Posons

$$u'_s = -\sum_{q=1}^{s-1} [(\overline{s-q}) + n\bar{q}],$$

$$u''_s = -\sum_{q=1}^{s-1} n\bar{q} \qquad \text{avec} \quad n\bar{q}(s-q) = 1.$$

On a d'une façon générale :

$$\sum_{q=1}^{s-1} \bar{q} = \sum_{q=1}^{s-1} (\overline{s-q}) = a_{s-1}^{(p-1)},$$

$a_{s-1}^{(p-1)}$ étant le symbole désignant la somme $\bar{1} + \bar{2} + \ldots + (\overline{s-1})$, donc

$$u'_s = \sum_{q=1}^{s-1} (\overline{s-q}) + n\bar{q} = -(n+1)\, a_{s-1}^{(p-1)}.$$

Par suite, on a

$$\sum_{s=2}^{p-2} u'_s x^{p-s} = -(n+1)\sum_{s=2}^{p-2} a_{s-1}^{(p-1)} x^{p-s}$$

$$= (n+1)\sum_{s=1}^{p-3} a_s^{(p-1)} x^{p-1-s}.$$

En effet, le développement de $\sum_{s=1}^{p-3}$ et de $\sum_{s=2}^{p-2}$ est le même dans les deux cas, et est exprimé par $\frac{1}{1}x^{p-2} + \frac{1}{2}x^{p-3} + \frac{1}{3}x^{p-4} + \ldots + \frac{1}{s-1}x^2$, mais

$$-(n+1)\sum_{s=1}^{p-3} a_s^{p-1} x^{p-1-s} = -(n+1)\,[g_{p-1}(x) - a_{p-2}^{(p-1)} x]$$

$$= -(n+1)\,[g_{p-1}(x) - x].$$

En effet,

$$\sum_{s=1}^{p-3} a_s^{(p-1)} x^{p-1-s} = \bar{1}\,x^{p-2} + (\bar{1}+\bar{2})\,x^{p-3} + \ldots + (\bar{1}+\bar{2}+\ldots+\overline{p-3})\,x^2,$$

$$g_{p-1}(x) = \bar{1}\,x^{p-2} + (\bar{1}+\bar{2})\,x^{p-3} + \ldots + 1 + 2 + \ldots + \overline{p-2})\,x,$$

donc

$$\sum_{s=2}^{p-2} u'_s x^{p-s} = -(n+1)\,g_{p-1}(x) + (n+1)\,x.$$

5. — L'égalité $n\bar{q}(s-q) = 1$ équivaut à $n(s-q) = q$, donc à $ns = (n+1)q$.

Si, pour un n tel que $1 \leqq n \leqq p-2$, s et q sont liés par cette égalité, $s = 0$ équivaut à $q = 0$, et $s = q = 0$ est le seul cas où $s = q$.

Si $s = 1$, donc $\neq 0$, on doit avoir $q \neq 0$ et $q \geqq 1 = s$, ce qui conduit à une impossibilité.

Si $s = p-1$, comme on a $q \leqq p-1 = s$ et comme $s \neq 0$, on a $s \neq q$. D'autre part, on peut écrire

$$q = (\overline{n+1})ns = (\overline{n+1})n(p-1) = -n(\overline{n+1}),$$

d'où $\quad n\bar{q} = n[-\bar{n}(n+1)] = -(n+1).$

Par suite,

$$\text{si} \quad s = 1, \quad \sum_{\substack{s=1 \\ s>q>0}} n\bar{q}x^{p-s} = 0;$$

$$\text{si} \quad s = p-1, \quad \sum_{\substack{s=p-1 \\ s>q>0}} n\bar{q}s^{p-s} = -(n+1)\,x.$$

Donc on a

$$\sum_{s=2}^{p-2} u''_s x^{p-s} + (n+1)x = - \sum_{\substack{1 \leqq s \leqq p-1 \\ q=(\overline{n+1})ns<s}} n\bar{q}x^{p-s}.$$

6. — En réunissant les résultats des paragraphes 4 et 5, on obtient

$$Q_n(x) = \sum_{s=2}^{p-2} u' x^{p-s} + \sum_{s=2}^{p-2} u''_s x^{p-s},$$

$$Q_n(x) = -(n+1)g_{p-1}(x) + (n+1)x - \sum n\bar{q}x^{p-s} - (n+1)x$$

$$= -(n+1)g_{p-1}(x) - \sum_{\substack{1 \leqq s \leqq p-1 \\ q=(\overline{n+1})ns<s}} n\bar{q}x^{p-s}$$

$$= -(n+1)g_{p-1}(x) - \sum_{\substack{1 \leqq s \leqq p-1 \\ q=(\overline{n+1})ns<s}} (n+1)\bar{s}x^{p-s}, \qquad \text{car} \quad n\bar{q} = (n+1)\bar{s}.$$

Donc, si l'on pose

$$P_u(x) = \sum_{\substack{1 \leqq s \leqq p-1 \\ (\overline{n+1})ns<s}} \bar{s}x^{p-1-s},$$

on a

$$Q_n(x) = -(n+1)\, g_{p-1}(x) - xP_n(x)(n+1)$$

et

$$P_n(x).x = -g_{p-1}(x) - (\overline{n+1})\, Q_n(x).$$

Les polynômes $P_n(x)$ sont les sommes de certains termes du polynôme fixe $f_{p-1}(x)$, d'une manière plus précise, d'une certaine moitié de ses termes, qui dépend de l'indice n. Ce résultat, qui se traduit par l'éclatement de la congruence fondamentale $f_{p-1}(x) = 0 \pmod p$ en $\frac{p-1}{2}$ congruences distinctes, pourrait revêtir une grande importance s'il ouvrait la possibilité d'appliquer à la théorie des congruences de Kummer les méthodes du type combinatoire.

Soit S_n l'ensemble des exposants s tels que $\bar{s}x^{p-s-1}$ soit un terme de $P_n(x)$, et soit T_n l'ensemble complémentaire de S_n dans la suite $= 1, 2, \ldots, (p-1)$. Montrons que $T_n = -S_n$, ce qui montrera que S_n a $\frac{p-1}{2}$ éléments. En effet, soit $s' = s$, alors on a $q' = (\overline{n+1})\, ns' = -(\overline{n+1})\, ns = -q$, et $s > q$ équivaut à $s' < q'$; autrement dit :

$$s \in S_n \iff s' \notin T_n.$$

et $T_n = -S_n$.

7. — Les $P_n(x)$ ne sont pas tous distincts, car $P_{\bar{n}}(x) = P_n(x)$.

En effet, considérons un $s = 0$, et soient

$$q = (\overline{n+1})\, ns \qquad \text{et} \qquad q' = (\overline{\bar{n}+1})\, \bar{n}s,$$
$$(\overline{\bar{n}+1})\, \bar{n}s = (\overline{n\bar{n}+\bar{n}})\, (n\bar{n})\, s = (\overline{n+1})\, s = \bar{n}q.$$

On a

$$s = (n+1)\, \bar{n}q = q + q'.$$

Soient s^*, q^*, q'^* les plus petits restes positifs mod p des s, q et q' considérés comme éléments de $\frac{Z}{p}$. On a

$$s^* = q^* + q'^*$$

ou

$$s^* = q^* + q'^* - p$$

selon que q est $< s$ ou $q > s$.

Or, dans le premier cas, $q'^* = sq^* - q^* < s^*$, d'où $q' < s$.

Dans le second cas, on a

$$q'^* - s^* = p^* - q^* > 0 \qquad \text{et} \qquad q' > s.$$

Ainsi $q < s$ équivaut à $q' < s$, et sx^{p-1-s} est un terme commun de $P_n(x)$ et de $P_{\bar{n}}(x)$, d'où résulte

$$P_{\bar{n}}(x) = P_n(x).$$

8. — Nous avons vu que tout $P_n(x)$ est une combinaison linéaire des $\frac{g_{p-1}(x)}{x} = \frac{f_{p-1}(x)}{x(x-1)}$ et des $\frac{Q_u(x)}{x}$, lesquels sont des combinaisons linéaires de

$$\frac{g_i(x)\, g_{p-i}(x)}{x} = \frac{f_i(x) f_{p-i}(x)}{x(x-1)^p}.$$

Vice versa, les $Q_n(x)$ sont des combinaisons linéaires des $g_{p-i}(x) = \frac{f_{p-1}(x)}{x-1}$ et des $xP_n(x)$ tandis que, puisque le vandermondien $|n^i|$ [$n = 2, 3, \ldots,$ $(p-2,\ i = 2, 3, \ldots, (p-2)$] n'est pas nul, les

$$g_i(x)\, g_{p-i}(x) = \frac{f_i(x) f_{p-i}(x)}{(x-1)^p}$$

sont des combinaisons linéaires des $Q_n(x)$. Par suite, tout élément t, distinct de 0 et de 1, de Ω_p ou d'une extension arbitraire de ce corps, est en même temps un zéro commun des $f_{p-1}(x)$ et $f_i(x) f_{p-1}(x)$ [$i = 2, 3, \ldots,$ $(p-2)$, on peut se limiter aux indices impairs] et zéro commun des $f_{p-1}(x)$ et $P_n(x)$ [$n = 2, 3, \ldots, (p-2)$, on peut, se limiter à un seul indice pour deux indices inverses dans Ω_p].

9. — Donc, si $t \equiv -\frac{b}{a} \pmod{p}$, où (a, b, c) est une solution de l'équation (F) telle que $abc \not\equiv 0 \bmod p$, t doit satisfaire aux congruences établies au paragraphe 6 :

$$\left.\begin{aligned} P_n(t) &= 0 \\ f_{p-1}(t) &= 0 \end{aligned}\right\} \bmod p, \qquad n = 2, 3, \ldots, (p-2),$$

et si t satisfait à ces congruences, il satisfait automatiquement à celles de MIRIMANOFF.

(Texte reçu le 31 janvier 1969.)

Paul LE LIDEC,
4, rue Lamothe-Guérin,
83-Toulon.