Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Marc Krasner

Travaux de P. Le Lidec sur une nouvelle forme des congruences de Kummer-Mirimanoff pour le premier cas du théorème de Fermat

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 6, n° 1 (1964-1965), exp. n° 5, p. 1-6

<http://www.numdam.org/item?id=SDPP_1964-1965__6_1_A4_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
6e année, 1964/65, n° 5

14 et 21 décembre 1964

TRAVAUX DE P. LE LIDEC
SUR UNE NOUVELLE FORME DES CONGRUENCES DE KUMMER-MIRIMANOFF POUR LE PREMIER CAS DU THÉORÈME DE FERMAT

par Marc KRASNER

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

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

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

$$\begin{aligned} &f_i(t)\, f_{p-i}(t) \equiv 0 \pmod p \qquad (i = 3 , 5 , \dots , p - 2) \\ &f_{p-1}(t) \equiv 0 \pmod p \end{aligned} \tag{M}$$

où

$$f_i(x) = \sum_{s=1}^{p-1} s^{i-1}\, x^{p-s} \qquad \text{et} \qquad t \equiv -\frac{b}{a} \pmod p \quad .$$

P. LE LIDEC a déduit de ces congruences d'autres congruences, équivalentes pour de tels t , et ayant une forme remarquable. Comme il s'agit, au fond, d'un calcul de polynômes dans le corps Ω_p de p éléments, nous n'écrirons, sauf à la fin, aucune congruence (mod p) , et les polynômes qu'on considèrera seront supposés appartenant à $\Omega_p[x]$. Mais, pour les besoins de la cause, nous munirons Ω_p de certaines autres structures et adopterons certains abus d'écriture. Premièrement, Ω_p sera considéré de la manière habituelle comme un $\mathbb{Z}$-module, où $\mathbb{Z}$ est l'anneau des entiers rationnels. Quand on écrira un entier rationnel n , ce signe, par abus d'écriture, signifiera le produit par n de l'unité I de Ω_p , $n.I = I + I + \dots + I$ (n fois) , tandis que, dans de rares cas où on en a besoin, l'entier rationnel n sera noté n^* . D'autre part, Ω_p sera considéré comme l'anneau quotient $\mathbb{Z}/(p)$ de $\mathbb{Z}$ par son idéal (p) , et 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. Enfin, Ω_p sera totalement ordonné par l'ordre des plus petits restes non-négatifs de ses éléments, considérés comme classes (mod p) dans $\mathbb{Z}$.

2. On a, visiblement, la formule de récurrence $f_{i+1}(x) = xf_i'(x)$ où $f'(x)$ désigne la dérivée de $f(x)$, et d'autre part, si $1 < i < p$,

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

tandis que

$$f_p(1) = \sum_{s=1}^{p-1} s^{p-1} = p - 1 \neq 0 \quad .$$

Par suite, si $2 \leqslant i \leqslant p - 1$ 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 $f_i(x)$ $(2 \leqslant i \leqslant p - 1)$ en $x - 1$ dans $\Omega_p[x]$ est $p - i$. Posons

$$g_i(x) = f_i(x)/(x - 1)^{p-i} = \sum_{q=1}^{i-1} a_q^{(i)} x^{i-q} \quad .$$

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

$$f_{p-1}(x) = \sum_{q=1}^{p-1} \bar{q}\, x^{p-q} \quad ,$$

donc

$$g_{p-1}(x)(x - 1) = \Big(\sum_{s=1}^{p-2} a_s^{(p-1)} x^{p-1-s}\Big)(x - 1) = \sum_{q=1}^{p-1} \bar{q}\, x^{p-q} \quad ,$$

ce qui donne $a_1^{(p-1)} = \bar{1} = 1$ et $a_q^{(p-1)} - a_{q-1}^{(p-1)} = \bar{q}$ $(2 \leqslant q \leqslant p - 1)$, d'où résulte $a_s^{(p-1)} = \sum_{q=1}^{s} \bar{q}$, et, en particulier,

$$a_{p-2}^{(p-1)} = \sum_{q=1}^{p-2} \bar{q} = -\,\overline{(p - 1)} = -\,(\overline{-1}) = 1 \quad .$$

Donc, on a

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

4. Calculons maintenant, pour $i = 2 , 3 , \ldots , p - 2$,

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

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

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

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

ce qui donne

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

5. n étant un entier tel que $1 \leqslant n \leqslant p-2$, posons

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

d'où

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

où

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

ou $(p-3)\,\dfrac{1}{s-q} = \dfrac{-3}{s-q}$ selon que $n\bar{q}(s-q) \neq$ ou $= 1$.

Or, $[n\bar{q}(s-q)]^{p-1} = 1$, donc, si $n\bar{q}(s-q) \neq 1$, on a

$$r_{s,q} = \frac{-1}{s-q} [n\bar{q}(s-q) + 1] = -\left(\overline{s-q} + n\bar{q}\right) \quad ,$$

et si $n\bar{q}(s-q) = 1$, on a $\overline{s-q} = n\bar{q}$, d'où résulte

$$r_{s,q} = \frac{-3}{s-q} = -\left(\overline{s-q} + n\bar{q} + n\bar{q}\right) \quad .$$

Posons

$$u'_s = -\sum_{q=1}^{s-1} \left(\overline{s-q} + n\bar{q}\right) \qquad \text{et} \qquad u''_s = \sum_{\substack{1 \leqslant q \leqslant s-1 \\ n\bar{q}(s-q)=1}} n\bar{q} \quad .$$

6. On a $\displaystyle\sum_{q=1}^{s-1} \bar{q} = \sum_{q=1}^{s-1} \overline{s-q} = a_{s-1}^{(p-1)}$, donc

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

Par suite, on a

$$\sum_{s=2}^{p-2} u'_s\, x^{p-s} = - (n + 1) \sum_{s=2}^{p-2} a_{s-1}^{(p-1)}\, x^{p-s} = - (n + 1) \sum_{s=1}^{p-3} a_s^{(p-1)}\, x^{p-1-s}$$

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

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

7. 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 $1 \leqslant n \leqslant p - 2$, s et q sont liés par cette égalité, $s = 0$ équivaut à $q = 0$, et $s = q = 0$ est le seul cas quand $s = q$. On a

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

Or supposons que $n\bar{q}(s - q) = 1$, et regardons ce qui se passe pour les valeurs $s = 1$ et $s = p - 1$. Si $s = 1$, donc $s \neq 0$, on a $q \neq 0$, donc $q \geqslant 1 = s$; et si $s = p - 1$, on a sûrement $q \leqslant p - 1 = s$, et puisque $s \neq 0$, on a $s \neq q$.

D'autre part, pour $s = p - 1$, on a $q = \overline{(n + 1)}ns = - n\overline{(n + 1)}$, d'où

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

Donc on a

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

8. En réunissant les résultats des paragraphes 6 et 7, on obtient

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

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

$$= - (n + 1)[g_{p-1}(x) - \sum_{\substack{1 \leqslant q \leqslant s \leqslant p-1 \\ ns = (n+1)q}} \bar{s} x^{p-s}] \quad ,$$

car $n\bar{q} = (n+1)\bar{s}$ si $n\bar{q}(s-q) = 1$. Donc, si l'on pose

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

on a

$$Q_n(x) = -(n+1)[g_{p-1}(x) + xP_n(x)] \quad \text{et} \quad xP_n(x) = -(\overline{n+1})\, Q_n(x) - g_{p-1}(x) .$$

9. 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 . Ceci est très curieux, et ouvre peut-être 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 $\bar{s}x^{p-s}$ soit un terme de $P_n(x)$, et soit T_n le complémentaire de S_n dans $\{1 , 2 , \dots , p-1\}$. Montrons que $T_n = -S_n$, ce qui montrera que S_n a $(p-1)/2$ 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, $s \in S_n \iff s' \in T_n$ et $T_n = -S_n$.

10. Les $P_n(x)$ ne sont pas tous distincts, car $P_{\bar{n}}(x) = P_n(x)$. En effet, considérons un $s \neq 0$, et soient

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

On a $s = (n+1)\bar{n}q = q + q'$. Soient s^* , q^* , q'^* les plus petits restes positifs (mod p) des s , q , q' considérés comme éléments de $\mathbb{Z}/(p)$. On a

$$s^* = q^* + q'^* \quad \text{ou} \quad s^* = q^* + q'^* - p \qquad \text{selon que} \quad q < s \quad \text{ou} \quad q > s .$$

Or, dans le premier cas, $q'^* = s - q^* < s$, d'où $q' < s$; et dans le second cas, on a $q'^* - s^* = p^* - q^* > 0$ et $q' > s$. Ainsi, $q < s$ équivaut à $q' < s$ et $\bar{s}x^{p-1-s}$ est un terme de $P_n(x)$ et de $P_{\bar{n}}(x)$ en même temps, d'où résulte $P_{\bar{n}}(x) = P_n(x)$.

11. Nous avons vu que tout $P_n(x)$ est une combinaison linéaire des

$$g_{p-1}(x)/x = f_{p-1}(x)/x(x-1) \qquad \text{et des} \qquad Q_n(x)/x ,$$

lesquels sont des combinaisons linéaires des

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

Vice versa, les $Q_n(x)$ sont des combinaisons linéaires des

$$g_{p-1}(x) = f_{p-1}(x)/(x-1) \qquad \text{et des} \qquad xP_n(x) \ ,$$

tandis que, puisque le vandermondien $|n^i|$ $(n = 2,3,\ldots,p-2\,;\ i=2,3,\ldots,p-2)$ n'est pas nul, les $g_i(x)\, g_{p-i}(x) = f_i(x)\, f_{p-i}(x)/(x-1)^p$ sont des combinaisons linéaires des $Q_n(x)x$. 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 $f_i(x)\, f_{p-i}(x)$ $(i = 2\ ,\ 3\ ,\ \ldots\ ,\ p-2$; 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 parmi deux indices inverses dans Ω_p).

12. Donc, si $t \equiv -a/b \pmod p$, où $(a\ ,\ b\ ,\ c)$ est une solution de l'équation (F) telle que $abc \not\equiv 0 \pmod p$, t doit satisfaire aux congruences de Le Lidec

$$\text{(LL)} \qquad \begin{aligned} &P_n(t) \equiv 0 \pmod p \qquad (n = 2\ ,\ 3\ ,\ \ldots\ ,\ p-2) \\ &f_{p-1}(t) \equiv 0 \pmod p \ , \end{aligned}$$

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