

MICHAEL BAUER

Sur les congruences identiques

Nouvelles annales de mathématiques 4^e série, tome 2
(1902), p. 256-264

http://www.numdam.org/item?id=NAM_1902_4_2__256_1

© Nouvelles annales de mathématiques, 1902, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

[13a]

SUR LES CONGRUENCES IDENTIQUES;

PAR M. MICHAEL BAUER, à Budapest.

D'après les éléments de la théorie des nombres, on sait que les nombres relatifs premiers avec n forment les racines de la congruence

$$(1) \quad x^{\varphi(n)} - 1 \equiv 0 \pmod{n}.$$

Si l'on désigne ces racines par les lettres

$$r_1, r_2, \dots, r_{\varphi(n)} \pmod{n},$$

il est évident que ces nombres forment aussi les racines de la congruence

$$(2) \quad \prod_{i=1}^{\varphi(n)} (x - r_i) \equiv 0 \pmod{n}.$$

Ainsi les congruences (1) et (2) ont les mêmes racines et le même degré. Enfin on sait que, si n est un nombre premier, on a

$$x^{p-1} - 1 \equiv \prod_{i=1}^{p-1} (x - r_i) \pmod{p}.$$

On peut se demander *pour quels modules on a la*

congruence identique

$$x^{\varphi(n)} - 1 \equiv \prod_{i=1}^{\varphi(n)} (x - r_i) \pmod{n}.$$

Cette question a été traitée par M. Gruber (1). Dans la présente Note, je donne une forme *explicite* de l'expression

$$\prod_{i=1}^{\varphi(n)} (x - r_i) \pmod{n}$$

et j'en tire quelques conséquences. Mes résultats sont les suivants :

Si p est un nombre premier impair et

$$n = p^\pi m \quad (m, p = 1),$$

on a la congruence identique

$$(I) \quad \prod_{i=1}^{\varphi(n)} (x - r_i) \equiv (x^{p-1} - 1)^{\frac{\varphi(n)}{p-1}} \pmod{p^\pi}.$$

Si $\beta > 1$ et

$$n = 2^\beta m, \quad m \equiv 1 \pmod{2},$$

on a la congruence identique

$$(II_a) \quad \prod_{i=1}^{\varphi(n)} (x - r_i) \equiv (x^2 - 1)^{\frac{\varphi(n)}{2}} \pmod{2^\beta}.$$

Cette dernière congruence peut être complétée par la suivante, qui est vraie pour tout module pair et dont la

(1) *Math. und naturwiss. Berichte aus Ungarn*, Bd XIII, p. 413-417.

vérité est évidente :

$$(II_b) \quad \prod_{i=1}^{\varphi(n)} (x - r_i) \equiv (x - 1)^{\varphi(n)} \pmod{2}$$

J'emploierai ces identités pour résoudre la question suivante :

d étant un diviseur de *n*, pour quelles valeurs de *d* et de *n* a-t-on la congruence identique

$$x^{\varphi(n)} - 1 \equiv \prod_{i=1}^{\varphi(n)} (x - r_i) \pmod{d}?$$

La Table suivante donne la réponse ; dans cette Table *p* désigne un nombre premier impair, *q* un nombre premier de la forme $2^k + 1$:

<i>d</i>	<i>n</i>
<i>p</i>	$p^2, 2p^2,$
2	$2^2, 2^2 \prod_s q_s$ (les facteurs q_s sont différents),
4	4,
$2q$	$2q.$

I.

1^o Soient

$$t_1, t_2, \dots, t_{(\varphi n)},$$

les nombres relatifs premiers avec *n*, qui sont $< n$, et introduisons l'expression

$$F_n(x) = \prod_{i=1}^{\varphi(n)} (x - t_i).$$

D'abord il est évident qu'on a

$$(3) \quad \left\{ \begin{array}{l} F_n(x) \equiv \prod_{i=1}^{\varphi(n)} (x - r_i) \pmod{n}, \\ F_p(x) = x^{p-1} - 1 + p \Phi(x), \\ F_2(x) = x - 1, \\ F_4(x) = (x-1)(x-3), \quad F_4(x) \equiv x^2 - 1 \pmod{4}, \\ F_n(x) \equiv (x-1)^{\varphi(n)} \pmod{2}, \quad n \equiv 0 \pmod{2}. \end{array} \right.$$

2° Nous démontrerons que

$$(4) \quad F_{p^\alpha}(x) \equiv (x^{p-1} - 1)^{p^{\alpha-1}} \pmod{p^\alpha}.$$

Avant tout nous prouverons l'identité

$$(5) \quad F_{p^{\beta+1}}(x) \equiv [F_{p^\beta}(x)]^p \pmod{p^\beta}.$$

Soient les nombres relatifs premiers avec p^β et $< p^\beta$

$$\tau_1, \tau_2, \dots, \tau_{\varphi(p^\beta)},$$

alors on a

$$F_{p^{\beta+1}}(x) = \prod_{m=0}^{p-1} (x - \tau_1 - mp^\beta)(x - \tau_2 - mp^\beta) \dots (x - \tau_{\varphi(p^\beta)} - mp^\beta).$$

Cependant

$$\begin{aligned} \prod_{i=1}^{\varphi(p^\beta)} (x - \tau_i - mp^\beta) &\equiv F_{p^\beta}(x) - mp^\beta \sum_i \frac{F_{p^\beta}'(x)}{x - \tau_i} \\ &\equiv F_{p^\beta}(x) - mp^\beta G(x) \pmod{p^{\beta+1}}, \end{aligned}$$

et ainsi

$$\begin{aligned} F_{p^{\beta+1}}(x) &\equiv \prod_{m=0}^{p-1} [F_{p^\beta}(x) - mp^\beta G(x)] \\ &\equiv [F_{p^\beta}(x)]^p - p^\beta G(x) [F_{p^\beta}(x)]^{p-1} \sum_{m=0}^{p-1} m \\ &\pmod{p^{\beta+1}}, \end{aligned}$$

d'où vient, puisque

$$\sum_{m=0}^{p-1} m = \frac{p(p-1)}{2}$$

que

$$(5) \quad F_{p^{\beta+1}}(x) \equiv [F_{p^{\beta}}(x)]^p \pmod{p^{\beta+1}}.$$

Cette identité donne d'abord

$$F_{p^2}(x) \equiv [F_p(x)]^p \equiv [(x^{p-1} - 1) + p \Phi(x)]^p \equiv (x^{p-1} - 1)^p \pmod{p^2}.$$

Supposons maintenant qu'on ait

$$F_{p^{\alpha-1}}(x) \equiv (x^{p-1} - 1)^{p^{\alpha-2}} \pmod{p^{\alpha-1}},$$

c'est-à-dire

$$F_{p^{\alpha-1}}(x) = (x^{p-1} - 1)^{p^{\alpha-2}} + p^{\alpha-1} \Phi_{\alpha-1}(x).$$

Alors on a, d'après (5)

$$F_{p^{\alpha}}(x) \equiv [F_{p^{\alpha-1}}(x)]^p \pmod{p^{\alpha}},$$

et ainsi

$$(4) \quad F_{p^{\alpha}}(x) \equiv (x^{p-1} - 1)^{p^{\alpha-1}} \pmod{p^{\alpha}}. \quad \text{c. q. f. d.}$$

3° Si $\beta > 1$, on a

$$(6) \quad F_{2^{\beta}}(x) \equiv (x^2 - 1)^{2^{\beta-2}} \pmod{2^{\beta}}.$$

Les nombres relatifs premiers avec $2^{\beta+1}$ sont

$$\begin{array}{ccccccc} 1, & 3, & 5, & \dots, & (2^{\beta} - 1) & & \\ -1, & -3, & -5, & \dots, & -(2^{\beta} - 1) & & \pmod{2^{\beta+1}}. \end{array}$$

De cette remarque suit immédiatement la congruence

$$(7) \quad F_{2^{\beta+1}}(x) \equiv F_{2^{\beta}}(x) F_{2^{\beta}}(-x) \pmod{2^{\beta+1}}.$$

Cependant

$$F_4(x) \equiv (x^2 - 1) \pmod{4}$$

et ainsi

$$F_{2^3}(x) \equiv [x^2 - 1 + 4\Psi(x)][x^2 - 1 + 4\Psi(-x)] \equiv (x^2 - 1)^2 \pmod{2^3},$$

Il est évident que de cette manière on a généralement

$$(6) \quad F_{2^{\beta}}(x) \equiv (x^2 - 1)^{2^{\beta-2}} \pmod{2^{\beta}}.$$

4° Si d est un diviseur du nombre n , on a

$$(8) \quad F_n(x) \equiv [F_d(x)]^{\frac{\varphi(n)}{\varphi(d)}} \pmod{d}.$$

Pour la démonstration, il suffit de remarquer que les nombres relatifs premiers avec n se trouvent dans les suites

$$dz + v_i,$$

où

$$v_1, v_2, \dots, v_{\varphi(d)}$$

désignent les nombres relatifs premiers avec d , qui sont $< d$. Chaque suite contient $\frac{\varphi(n)}{\varphi(d)}$ nombres (n) , qui sont relatifs premiers avec n . L'identité (8) donne, avec les précédentes, les formules (I), (II_a), (II_b).

II.

1° Soit d un diviseur de n ; quand a-t-on la congruence identique

$$(a) \quad x^{\varphi(n)} - 1 \equiv \prod_{i=1}^{\varphi(n)} (x - r_i) \pmod{d}?$$

Si la congruence (a) est vraie pour un module d , elle est aussi vraie pour chaque diviseur de d .

Examinons donc la congruence identique

$$(b) \quad x^{\varphi(n)} - 1 \equiv \prod_{i=1}^{\varphi(n)} (x - r_i) \pmod{p}.$$

(262)

Cette congruence est équivalente d'après (I) à la congruence

$$(b') \quad (x^{p-1} - 1)^{\frac{\varphi(n)}{p-1}} \equiv x^{\varphi(n)} - 1 \pmod{p}$$

et ainsi, il faut qu'on ait

$$(-1)^{\frac{\varphi(n)}{p-1}} \equiv -1 \pmod{p},$$

d'où résulte

$$n = \begin{cases} p^\alpha, \\ 2p^\alpha. \end{cases}$$

D'autre part, si n prend ces valeurs, il est évident qu'on a la congruence (b).

2° On n'a jamais la congruence identique

$$(c) \quad x^{\varphi(n)} - 1 \equiv \prod_{i=1}^{\varphi(n)} (x - r_i) \pmod{p^2}.$$

Les valeurs de n , que nous avons trouvées possibles, sont $n = \begin{cases} p^\alpha \\ 2p^\alpha \end{cases}$; on a dans ces cas

$$(d) \quad \prod_{i=1}^{\varphi(n)} (x - r_i) \equiv (x^{p-1} - 1)^{p^{\alpha-1}} \pmod{p^2}.$$

Où $\alpha < 1$ et ainsi

$$(x^{p-1} - 1)^{p^{\alpha-2}} = x^{p^{\alpha-2}(p-1)} - 1 + p f(x).$$

d'où vient

$$(x^{p-1} - 1)^{p^{\alpha-1}} \equiv (x^{p^{\alpha-2}(p-1)} - 1)^p \pmod{p^2}.$$

Donc $\prod_{i=1}^{\varphi(n)} (x - r_i)$ n'est pas congru avec l'expression

$$x^{p^{\alpha-1}(p-1)} - 1 \pmod{p^2}.$$

3° Examinons la congruence identique

$$(e) \quad x^{\varphi(n)} - 1 \equiv \prod_{i=1}^{\varphi(n)} (x - r_i) \equiv (x - 1)^{\varphi(n)} \pmod{2}.$$

Soit

$$\varphi(n) = 2^h l, \quad l \equiv 1 \pmod{2}.$$

Nous verrons que la congruence (e) n'est vraie que dans le cas où $l = 1$. D'une induction totale suit d'abord

$$(x - 1)^{2^h} \equiv (x^{2^h} - 1) \pmod{2},$$

et si l'on pose

$$x^{2^h} = y,$$

la congruence (e) est équivalente à celle-ci :

$$(y - 1)^l \equiv y^l - 1 \pmod{2}, \quad l \equiv 1 \pmod{2},$$

qui est seulement vraie dans le cas où $l = 1$. Ainsi nous avons $\varphi(n) = 2^h$, d'où résulte

$$n = \begin{cases} 2^{\alpha}, \\ 2^{\alpha} \prod_s q_s \end{cases} \quad (\text{les facteurs } q_s \text{ sont différents}).$$

4° La congruence identique

$$(f) \quad x^{\varphi(n)} - 1 \equiv \prod_{i=1}^{\varphi(n)} (x - r_i) \pmod{4}$$

est seulement vraie dans le cas où $n = 4$. Les valeurs n , que nous avons trouvées possibles, peuvent être classées de la manière suivante :

$$n = \begin{cases} 4, \\ 2^{\beta} \\ 2^{\beta} \prod_s q_s \end{cases} \quad \begin{cases} (\beta > 2), \\ (\beta \geq 2). \end{cases}$$

(264)

On a dans le premier cas

$$x^2 - 1 \equiv (x - 1)(x - 3) \pmod{4}.$$

On a dans les autres cas

$$\varphi(n) = 2^h \quad (h > 1),$$

en conséquence

$$\prod_{i=1}^{\varphi(n)} (x - r_i) \equiv (x^2 - 1)^{2^{h-1}} \pmod{4}, \quad [h - 1 > 0].$$

Or

$$(x^2 - 1)^{2^{h-1}} = x^{2^{h-1}} - 1 + 2g(x),$$

et ainsi

$$\prod_{i=1}^{\varphi(n)} (x - r_i) \equiv (x^{2^{h-1}} - 1)^2 \pmod{4}.$$

Donc $\prod_{i=1}^{\varphi(n)} (x - r_i)$ n'est pas congru avec l'expression $x^{2^h} - 1 \pmod{4}$.

5° Il reste encore à discuter le cas $d = 2p$. On voit d'après les précédents que la congruence identique

$$x^{\varphi(n)} - 1 \equiv \prod_{i=1}^{\varphi(n)} (x - r_i) \pmod{2p}$$

ne peut être vraie que pour

$$p = q, \quad n = 2q,$$

et que, dans ce cas, on a véritablement

$$x^{\varphi(2q)} - 1 \equiv \prod_{i=1}^{\varphi(2q)} (x - r_i) \pmod{2q}.$$
