NOUVELLES ANNALES DE MATHÉMATIQUES

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>

[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

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

Si l'on désigne ces racines par les lettres

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

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

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

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

$$n = p^{\pi} m \qquad (m, p = 1),$$

on a la congruence identique

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

Si $\beta > 1$ *et*

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

on a la congruence identique

$$(\mathrm{II}_a) \qquad \prod_{i=1}^{\varphi(n)} (x - r_i) \equiv (x^2 - 1)^{\frac{\varphi(n)}{2}} \pmod{2^{\beta}}.$$

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 :

$$(\mathrm{II}_b) \qquad \prod_{i=1}^{\varphi(n)} (x - r_i) \equiv (x-1)^{\varphi(n)} \pmod 2$$

J'emploirai 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 $2^k + 1$:

d	n	
p	p^α, $2p^\alpha$,	
2	2^α, $2^\alpha \prod_s q_s$	(les facteurs q_s sont différents),
4	4,	
$2q$	$2q$.	

1.

1° Soient

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

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

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

D'abord il est évident qu'on a

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

2° Nous démontrerons que

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

Avant tout nous prouverons l'identité

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

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

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

alors on a

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

Cependant

$$\prod_{i=1}^{\varphi(p^\beta)} (x - \tau_i - mp^\beta) \equiv F_{p^\beta}(x) - mp^\beta \sum_i \frac{F_{p^\beta}(x)}{x - \tau_i}$$

$$\equiv F_{p^\beta}(x) - mp^\beta\, G(x) \pmod{p^{\beta+1}},$$

et ainsi

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

$$\equiv [F_{p^\beta}(x)]^p - p^\beta\, G(x)\,[F_{p^\beta}(x)]^{p-1} \sum_{m=0}^{p-1} m$$

$$\pmod{p^{\beta+1}},$$

d'où vient, puisque

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

que

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

Cette identité donne d'abord

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

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

$$(4) \qquad F_{p^\alpha}(x) \equiv (x^{p-1}-1)^{p^{\alpha-1}} \pmod{p^\alpha}. \qquad \text{C. Q. F. D.}$$

3° Si $\beta > 1$, on a

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

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

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

De cette remarque suit immédiatement la congruence

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

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

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

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

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

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

$$dz + v_i,$$

où

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

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*

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

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

Examinons donc la congruence identique

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

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

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

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

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

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

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

Or $\alpha < 1$ et ainsi

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

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

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

Soit

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

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 :

$$(y-1)^l \equiv y^l - 1 \pmod 2, \qquad l \equiv 1 \pmod 2,$$

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

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

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

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

On a dans le premier cas

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

On a dans les autres cas

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

en conséquence

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

Or

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

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

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

et que, dans ce cas, on a véritablement

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