BOLLETTINO UNIONE MATEMATICA ITALIANA

GIOVANNI SANSONE

La risoluzione apiristica delle congruenze cubiche

Bollettino dell'Unione Matematica Italiana, Serie 1,
Vol. 7 (1928), n.1, p. 27-32.

Unione Matematica Italiana

<[http:
//www.bdim.eu/item?id=BUMI_1928_1_7_1_27_0](http://www.bdim.eu/item?id=BUMI_1928_1_7_1_27_0)>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

Bollettino dell'Unione Matematica Italiana, Unione
Matematica Italiana, 1928.

La risoluzione apiristica delle congruenze cubiche ⁽¹⁾.

Nota di GIOVANNI SANSONE (a Firenze).

Il prof. M. CIPOLLA con una brillante serie di Note ⁽²⁾ riuscì a stabilire una formula di risoluzione apiristica delle congruenze binomie. Successivamente il prof. G. SCORZA ⁽³⁾, facendo uso della formula di interpolazione di LAGRANGE, diede in una sua Nota in modo suggestivo ragione della struttura della formula del prof. CIPOLLA. Per le congruenze binomie di grado e modulo potenza di un numero primo il prof. G. MIGNOSI ⁽⁴⁾ mercè l'impiego della serie binomiale pervenne con procedimento elegante alla costruzione di una loro formula risolutiva.

La lettura di queste interessanti note ci spinse a studiare il problema della risoluzione delle congruenze di terzo e quarto

⁽¹⁾ La memoria sarà pubblicata negli « Annali di Matematica ».

⁽²⁾ M. CIPOLLA: a) *Formule di risoluzione della congruenza binomia quadratica e biquadratica*. (« Rend. della R. Acc. delle Scienze fis. e mat. di Napoli », gennaio 1905); b) *Sulla risoluzione apiristica delle congruenze binomie secondo un modulo primo*. (« Math. Ann. », Bd. L. XIII. 1906); c) *Sulla risoluzione apiristica delle congruenze binomie*. Note 1^a e 2^a (« Rend. della R. Acc. Naz. dei Lincei », fasc. 8^o e 9^o del vol. XVI della serie 5^a, 1^o sem. 1927).

⁽³⁾ G. SCORZA: *La risoluzione apiristica delle congruenze binomie e la formula di interpolazione di Lagrange*. (« Rend. della R. Acc. Naz. dei Lincei », fasc. 7^o, vol. III, 1^o sem. 1926).

⁽⁴⁾ G. MIGNOSI: *La convergenza in un campo di integrità finito e la risoluzione apiristica delle congruenze binomie*. (« Rend. del Circ. Mat. di Palermo, t. L. 1926).

grado e qui, in questo riassunto, esponiamo quanto riguarda la risoluzione delle congruenze di terzo grado (1).

La questione sembra assai facile, perchè è da presumere che sia possibile superarne le difficoltà trasportando in un campo di integrità finito qualcuno dei noti procedimenti per la risoluzione delle equazioni cubiche (2), ma ciascuno di questi procedimenti suppone l'esistenza di una radice cubica dell'unità, mentre la congruenza

$$x^3 + x + 1 \equiv 0 \pmod{p}$$

è impossibile, anche nel campo di GAUSS, per p della forma $12k + 5$.

Ne segue che lo studio generale delle congruenze cubiche richiede una trattazione diretta, e qui vogliamo indicare i risultati conseguiti.

Data una congruenza cubica rispetto ad un modulo primo p , con $p \neq 2, 3$, essa può sempre ridursi con una conveniente trasformazione lineare o ad una congruenza binomia, o ad una congruenza del tipo:

$$(1) \quad x^3 + ax + a \equiv 0 \pmod{p}; \quad [a \mid 0].$$

Posto:

$$D_0(a) = 1, \quad D_1(a) = 0, \quad D_2(a) = a.$$

$$D_{2r}(a) = \binom{k}{0} a^k - \binom{k-1}{2} a^{k-1} + \binom{k-2}{4} a^{k-2} - \binom{k-3}{6} a^{k-3} + \dots + \\ + (-1)^r \binom{k-r}{2r} a^{k-r}; \quad k-1:$$

(1) I risultati relativi alle congruenze biquadratiche sono contenuti in una Nota in pubblicazione nei « Rend. della R. Acc. dei Lincei »: faremo fra poco tempo noti i risultati relativi alle più generali congruenze di quarto grado.

(2) Il prof. U. SCARPIS in una sua Nota: *Intorno alla risoluzione per radicali di un'equazione algebrica in un campo di Galois* (« Periodico di Matematiche », ser. III, vol. IX, p. 73, 1911) cercò di applicare la formula cardanica alla risoluzione di una congruenza cubica e constatò che in certi casi essa diventa illusoria quando la congruenza ammette tre radici ed efficace quando ne possiede una sola, mentre in certi casi succede il contrario, ma non si pose la questione generale della risoluzione delle congruenze cubiche. In un successivo lavoro: *Intorno all'interpretazione della teoria di Galois in un campo di razionalità finito* (« Annali di Matematica », t. XXIII, ser. III, 1914) prese in generale a studiare le congruenze col proposito di accennare alle modificazioni che potrebbe subire la teoria di GALOIS ove si volesse applicare ad equazioni di un campo finito di integrità. Convien però a questo proposito notare che abbiamo costruito la formula apiristica di risoluzione di una congruenza cubica anche nel caso di un modulo primo della forma $12k + 5$, mentre in questo caso la sua risoluzione non può farsi dipendere dalla risoluzione di congruenze binomie.

con

$$r = \left\lfloor \frac{k}{3} \right\rfloor,$$

e

$$D_{2k+1}(a) = -\binom{k}{1}a^k + \binom{k-1}{3}a^{k-1} - \binom{k-2}{5}a^{k-2} + \binom{k-3}{7}a^{k-3} - \dots + (-1)^{r+1} \binom{k-r}{2r+1}a^{k-r}; \quad k \geq 1;$$

con

$$r = \left\lfloor \frac{k-1}{3} \right\rfloor.$$

troviamo che la congruenza (1) ha tre radici incongrue modulo p allora e allora soltanto che sia:

$$(2) \quad D_{p-2}(a) \equiv 0 \pmod{p} \quad [a \not\equiv 0].$$

La congruenza (1) ha una e una sola radice allora soltanto che si abbia $4a + 27 \equiv 0 \pmod{p}$ e il valore del polinomio

$$\psi(a) = [4a^\delta + \sum_1^\delta 2c_r a^{\delta-r}] [4a + 27]^{p-2}$$

con $\delta = \frac{p-2}{3}$ se $p = 6h + 5$ e $\delta = \frac{p-1}{3}$ se $p = 6h + 7$, e con

$$c_r = (-1)^r \begin{vmatrix} \binom{\frac{p-3}{2}}{0} & 0 & 0 & \dots & 0 & \binom{\frac{p-3}{2}-1}{1} \\ \binom{\frac{p-3}{2}-1}{2} \binom{\frac{p-3}{2}}{0} & 0 & \dots & 0 & \binom{\frac{p-3}{2}-2}{3} \\ \binom{\frac{p-3}{2}-2}{4} \binom{\frac{p-3}{2}-1}{2} \binom{\frac{p-3}{2}}{0} & \dots & 0 & \binom{\frac{p-3}{2}-3}{5} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \binom{\frac{p-3}{2}-(r-1)}{2(r-1)} \binom{\frac{p-3}{2}-(r-2)}{2(r-2)} \dots & \dots & \binom{\frac{p-3}{2}}{0} \binom{\frac{p-3}{2}-r}{2r-1} \\ \binom{\frac{p-3}{2}-r}{2r} \binom{\frac{p-3}{2}-(r-1)}{2(r-1)} \dots \binom{\frac{p-3}{2}-1}{2} \binom{\frac{p-3}{2}-(r+1)}{2r+1} \end{vmatrix}$$

soddisfa la congruenza:

$$(3) \quad [27 + 4a]\psi^3(a) - [27 + 4a]a^\delta\psi(a) + [9+a]a^{2\delta}\psi(a) - a^{3\delta} = 0 \pmod{p}.$$

La soluzione della congruenza proposta è data dalla formula:

$$x \equiv -[a^{\delta} - 3\psi(a)]/[a^{\delta} - 2\psi(a)].$$

Infine la congruenza (1) è impossibile per tutti i valori di a che non soddisfano nè la (2) nè la (3) e non siano congrui con lo 0 e $-\frac{27}{4}$ modulo p .

Quando la (1) abbia tre radici incongrue, col metodo del prof. SCORZA si indica il procedimento per la costruzione di tutte le formule risolutive della congruenza (1), in numero di 3^h , essendo $h = \frac{p-5}{6}$ se $p \equiv 5 \pmod{6}$ e $h = \frac{p-7}{6}$ se $p \equiv 1 \pmod{6}$.

Si presenta poi la maggiore questione di assegnare in funzione esplicita di a una formula risolutiva della (1) nel caso che essa abbia tre radici: si ottiene allora il semplicissimo risultato. Se le tre radici della (1) non hanno lo stesso carattere quadratico modulo p , quella radice che non ha il carattere delle altre due è data dalla formula:

$$(4) \quad x \equiv (-1)^{\frac{p-3}{2}} D_{\frac{p-3}{2}}(a) D_{\frac{p-5}{2}}(a) \pmod{p}.$$

Si ha contemporaneamente il seguente risultato fondamentale per la risoluzione delle congruenze di quarto grado: la congruenza (1) ha tre radici che hanno lo stesso carattere quadratico mod. p , allora e allora soltanto che si abbia:

$$(-1)^{\frac{p+1}{2}} D_{\frac{p-3}{2}}(a) + \frac{3}{2} D_{\frac{p-5}{2}}(a) \equiv 0 \pmod{p}.$$

Quando la (1) abbia tre radici con lo stesso carattere quadratico modulo p , indichiamo la forma da assegnare ad una trasformazione lineare, perchè la (1) si muti in un'altra congruenza dello stesso tipo le cui tre radici non abbiano lo stesso carattere quadratico modulo p , e perciò risolubile con la (4).

Determinata con la (4) una radice x_1 della (1), le altre due radici x_2 e x_3 si determinano con le formule:

$$2x_2 \equiv \frac{k}{f'(x_1)} - x_1, \quad 2x_3 \equiv -\frac{k}{f'(x_1)} - x_1 \pmod{p},$$

essendo

$$f(x) = x^3 + ax + a, \quad e \quad k^2 \equiv -a^2(4a + 27) \pmod{p}.$$

Prendiamo poi a studiare particolarmente il caso $p = 6h + 7$, e sempre nella ipotesi che la (1) abbia tre radici, dimostriamo che se per x prendiamo una radice della congruenza (possibile)

$$a - 9x - 3x^2 \equiv 0 \pmod{p},$$

la trasformazione lineare

$$(5) \quad x = (xy + 1) / \left(y + \frac{9x - 2a}{a(2x + 3)} \right)$$

muta la (1) nella congruenza binomia:

$$(6) \quad y^3 + \frac{(27 + 4a)(2a - 9x)}{a^2(2x + 3)^3} \equiv 0 \pmod{p}$$

risolvibile colla formula del prof. CIPOLLA.

Sempre nel caso $p = 6h + 7$ e nelle ipotesi 1°) che le tre radici della (1) non abbiano lo stesso carattere cubico, cioè per a valgono le relazioni:

$$D_{\frac{p-4}{3}}(a) \not\equiv 0, \quad D_{\frac{p-7}{3}}(a) \equiv 0 \pmod{p}.$$

2°) che per il numero a si abbia

$$3D_{\frac{p-10}{3}}(a) \equiv 2(-1)^{\frac{p+2}{3}} D_{\frac{p-7}{3}}(a) \pmod{p}.$$

allora il numero x dato dalla formula:

$$(7) \quad x \equiv (-1)^{\frac{p+2}{3}} D_{\frac{p-4}{3}}(a) / D_{\frac{p-7}{3}}(a) \pmod{p}$$

è una radice della congruenza (1).

Se abbiamo invece:

$$D_{\frac{p-4}{3}}(a) \equiv 0, \quad D_{\frac{p-7}{3}}(a) \not\equiv 0, \quad 3D_{\frac{p-10}{3}}(a) \equiv 2(-1)^{\frac{p+2}{3}} D_{\frac{p-7}{3}}(a) \pmod{p},$$

allora, se nella (5) poniamo il valore di x fornito dalla (7), la (1) si trasforma nella congruenza binomia (6).

Diamo infine la risoluzione delle congruenze binomie cubiche rispetto ai moduli p^n ; qui abbiamo fatto notare esplicitamente come data una radice semplice x della congruenza $f(x) \equiv 0 \pmod{p}$, l'ordinario metodo di NEWTON per la risoluzione numerica approssimata delle equazioni algebriche, applicato alla radice x successivamente 1. 2. 3. ... volte, permette di costruire una radice della congruenza $f(x) \equiv 0$ rispettivamente per i moduli $p^2, p^3, p^4, \dots$.

Abbiamo fatto seguire al lavoro due *Tavole numeriche* per la risoluzione delle congruenze cubiche col modulo p primo inferiore a 100, le quali ammettono tre radici oppure una sola.

Firenze, novembre 1927.