Bollettino
Unione Matematica
Italiana

Giovanni Sansone

Sul problema della risoluzione apiristica delle congruenze di grado qualunque rispetto ad un modulo primo e la risoluzione apiristica delle congruenze di quarto grado

Bollettino dell'Unione Matematica Italiana, Serie 1, Vol. **7** (1928), n.3, p. 127–133.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1928_1_7_3_127_0>

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

Sul problema della risoluzione apiristica delle congruenze di grado qualunque rispetto ad un modulo primo, e la risoluzione apiristica delle congruenze di quarto grado.

Nota di G. SANSONE (a Firenze).

1. Abbiamo riassunto in una Nota di questo Bollettino (1) i nostri studi sulle congruenze cubiche, ora daremo conto dei risultati sulle congruenze di grado superiore e in particolare sulle congruenze di quarto grado.

a) Per la determinazione del numero delle radici di una congruenza è noto il criterio di RADOS (2): Data la congruenza

$$(1) \qquad f(x) = a_0 x^{p-2} + a_1 x^{p-3} + \ldots + a_{p-3} x + a_{p-2} \equiv 0 \pmod{p}$$

con $a_0, a_1, \ldots, a_{p-2}$ interi assoluti, p primo dispari, $a_{p-2} \not\equiv 0 \pmod{p}$, si ponga $a_{m+p-1} = a_m$ e si consideri il determinante *di ordine* $p-1$

$$D = |a_{m+n}| \qquad m, n = 0, 1, 2, \ldots, p-2.$$

(1) Questo « Bollettino », Anno VII, n. 1, p. 27. Il lavoro riassunto in questa nota sarà presentato per la pubblicazione nelle « Memorie della R. Acc. Naz. dei Lincei ».

(2) G. RADOS, *Zur Theorie der congruenzen höheren Grades.* « Journ. für die r. und ang. Math. », B. 99; p. 258-260.

Condizione necessaria e sufficiente perchè la (1) abbia k radici distinte è che la caratteristica del determinante D modulo p sia uguale a $p - 1 - k$.

Abbiamo dimostrato che al criterio ora enunciato si può sostituire il seguente, il quale fa invece intervenire la caratteristica aritmetica di un determinante di *ordine uguale al grado della congruenza.*

Data la congruenza

$$(2) \qquad f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n \equiv 0 \pmod{p}$$

priva di radici multiple, si formi col procedimento del TRUDI [1] il resto della divisione di x^h per $f(x)$ e sia esso

$$R_h(x) = A_{1,h} x^{n-1} + A_{2,h} x^{n-2} + \ldots + A_{n-1,h} x + A_{n,h}, \qquad h = n, n+1, \ldots.$$

[I coefficienti $A_{i,h}$ possono esprimersi con determinanti formati coi coefficienti a della congruenza]. Formiamo il determinante di ordine n:

$$M = \begin{vmatrix} A_{1,p-1} & A_{2,p-1} & \ldots & A_{n-1,p-1} & A_{n,p-1}-1 \\ A_{1,p} & A_{2,p} & \ldots & A_{n-1,p}-1 & A_{n,p} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ A_{1,p+n-3} & A_{2,p+n-3}-1 & \ldots & A_{n-1,p+n-3} & A_{n,p+n-3} \\ A_{1,p+n-2}-1 & A_{2,p+n-2} & \ldots & A_{n-1,p+n-2} & A_{n,p+n-2} \end{vmatrix}$$

Condizione necessaria e sufficiente perchè la congruenza (2) abbia k radici incongrue e k soltanto è che la caratteristica aritmetica del determinante M sia uguale ad $n - k$.

b) La risoluzione di una congruenza può farsi dipendere dalla risoluzione di un'altra avente le sue radici tutte con lo stesso carattere quadratico, o cubico,... o m^{esimo} rispetto al modulo [m divisore di $p - 1$].

Se la congruenza (2) ammette le n radici incongrue $x_1, x_2, \ldots, x_n$ aventi lo stesso carattere m^{esimo} modulo p (m divisore di $p - 1$), si può effettuare l'abbassamento del grado della congruenza tutte le volte che si sappia determinare un numero α per il quale ***non*** si abbia simultaneamente

$$\left[\frac{x_1 + \alpha}{p}\right]_m = \left[\frac{x_2 + \alpha}{p}\right]_m = \ldots = \left[\frac{x_n + \alpha}{p}\right]_m.$$

In un prossimo lavoro mostreremo come questo procedimento conduca per le congruenze cubiche e senza eccezioni a nuove no-

[1] N. TRUDI, *Teoria dei determinanti e loro applicazioni.* [Napoli, 1862], p. 122 e seg.

tevoli formule risolutive i cui termini si esprimono per mezzo di polinomi soddisfacenti a congruenze differenziali del secondo ordine modulo p.

c) La congruenza

$$x^{k+1} + a_1x^k + a_2x^{k-1} + \dots + a_kx + a_{k+1} \equiv 0 \pmod{p}$$

abbia $k+1$ radici incongrue α, x_1, x_2,..... x_k e si abbia:

$$\left[\frac{\alpha}{p}\right]_m = r, \quad \left[\frac{x_1}{p}\right]_m = s_1, \quad \left[\frac{x_2}{p}\right]_m = s_2, \dots \left[\frac{x_k}{p}\right]_m = s_k$$

[m divisore di $p-1$] con $r \equiv s_1, s_2, \dots, s_k \pmod{p}$. Se i numeri $s_1, s_2, \dots, s_k$ coincidono consideriamo il binomio $x^m - s_1$, se non coincidono consideriamo il prodotto $P(x) = (x^m - s_1)(x^m - s_2)\dots$ esteso a tutti i numeri s incongrui modulo p. Col procedimento del TRUDI determiniamo il resto della divisione di $P(x)$ per $f(x)$ e sia esso $A_1x^k + A_2x^{k-1} + \dots + A_{k+1}$.

È $A_1 \equiv 0 \pmod{p}$ e la radice α è espressa dalla relazione:

$$\alpha \equiv A_2 A_1 - a_1 \pmod{p}.$$

2. Abbiamo preso a considerare le congruenze di quarto grado e ci siamo dapprima attenuti ai procedimenti classici di FERRARI e di EULERO per ottenere la loro risoluzione.

Si dimostra:

a) Data la congruenza

$$x^4 + ax^2 + bx + c \equiv 0 \pmod{p} \tag{3}$$

con a, b, c, d interi assoluti, p primo, $p \equiv 2, 3$, supposto che essa abbia 4 radici incongrue α, β, γ, δ, i tre numeri

$$y_1 = [(\alpha+\beta)-(\gamma+\delta)]^2, \quad y_2 = [(\alpha+\gamma)-(\beta+\delta)]^2, \quad y_3 = [(\alpha+\delta)-(\beta+\gamma)]^2$$

sono radici della congruenza cubica

$$y^3 + 8ay^2 + (16a^2 - 64c)y - 64b^2 \equiv 0 \pmod{p} \tag{4}$$

la quale deve ammettere tre radici residuo quadratico del modulo p. [La (4) con la trasformazione $y = 2^4t$ è la risolvente di EULERO della (3)]. Questo accadrà allora soltanto che i numeri

$$a_1 = 8a, \quad a_2 = 16a^2 - 64c, \quad a_3 = -64b^2$$

soddisfino le tre condizioni:

$$\begin{gathered} D_{\frac{p-3}{2}}(a_1, a_2, a_3) \equiv 0, \quad D_{\frac{p-5}{2}}(a_1, a_2, a_3) \equiv 0, \\ a_3 D_{\frac{p-7}{2}}(a_1, a_2, a_3) \equiv \pm 1 \end{gathered} \pmod{p} \tag{5}$$

dove con $D_l(a_1, a_2, a_3)$ indichiamo un polinomio isobarico di peso l definito dalla relazione

$$(-1)^{\left[\frac{l}{2}\right]} D_l(a_1, a_2, a_3) = \sum_{i,r} (-1)^{r+i} \binom{l-r-i}{r-i} \binom{r-i}{2i} a_1^{\,l-2r} a_2^{\,r-3i} a_3^{\,2i} +$$

$$+ \sum_{i,r} (-1)^{r+i} \binom{l-r-i-2}{r-i+1} \binom{r-i+1}{2i+1} a_1^{\,l-2r-3} a_2^{\,r-3i} a_3^{\,2i+1}$$

essendo le due somme estese a tutti i possibili numeri interi non negativi i, r, per i quali i termini dei coefficienti binomiali risultino non negativi e i numeratori maggiori o uguali ai denominatori, con la solita convenzione per il simbolo $\binom{a}{o}$, cioè $\binom{a}{o} = 1$.

b) Determinate le condizioni (5) le quali ci assicurano che la (3) ha quattro radici, per costruirle abbiamo preso per incognite i tre numeri

$$z_1 = \beta\gamma + \alpha\delta, \quad z_2 = \gamma\alpha + \beta\delta, \quad z_3 = \alpha\beta + \gamma\delta$$

e formata la risolvente cubica della (3)

$$z^3 - az^2 - 4cz - (b^2 - 4ac) \equiv 0 \pmod{p} \tag{6}$$

[la quale con la trasformazione $z = 2\mu$ è la risolvente di FERRARI della (3)].

Per trovare le radici della (3) basta saper trovare una radice della (6), ciò che allo stato dei nostri studi sappiamo ottenere in due casi:

1°) per $b^2 - 4ac = 0$; basterà prendere $z \equiv 0$ (cosa ovvia);

2°) quando i tre numeri z_1, z_2, z_3 non hanno lo stesso carattere quadratico modulo p, quello di essi che non ha il carattere quadratico degli altri due si determina con la formula

$$z \equiv (-1)^{\frac{p-3}{2}} D_{\frac{p-3}{2}}(\alpha_1, \alpha_2, \alpha_3) / D_{\frac{p-5}{2}}(\alpha_1, \alpha_2, \alpha_3) \pmod{p}$$

con $\alpha_1 = -a, \quad \alpha_2 = -4c, \quad \alpha_3 = -(b^2 - 4ac)$.

3. Per approfondire lo studio della (3) abbiamo voluto trovare in quali casi essa ha radici multiple. Riducendola (con una trasformazione a radici multiple) alla forma

$$x^4 + ax^2 + bx + b \equiv 0 \pmod{p} \tag{7}$$

si trova:

1°) $a \equiv b \equiv 0$, $x \equiv 0$ è radice quadrupla;

2°) $b \equiv 0$, $a \not\equiv 0$, $x \equiv 0$ è radice doppia, e soltanto per $\left(\frac{-a}{p}\right) = 1$ essa ammette altre due radici semplici;

3°) $a \equiv 0$, $b \not\equiv 0$ essa ha radici multiple soltanto per $b \equiv 2^8/3^3$ e in questo caso ha la radice doppia $x \equiv -4/3$. Vi sono ancora due altre radici semplici per $\left(\frac{-2}{p}\right) = 1$;

4°) $ab \not\equiv 0$, $(a^2 + 12b)(2a^3 - 8ab + 9b^2) \equiv 0 \pmod{p}$ la congruenza ha radici multiple soltanto per $a \equiv -2^7/3$, $b \equiv -2^{12}/3$, e in questo caso possiede la radice $-2^2/3$ tripla e la radice 2^3 semplice;

5°) $ab(a^2 + 12b)(2a^3 - 8ab + 9b^2) \not\equiv 0 \pmod{p}$ la congruenza ha radici multiple soltanto per

$$16a^4b - 4a^3b^2 - 128a^2b^2 + 144ab^3 + 256b^3 - 27b^4 \equiv 0 \pmod{p}$$

[si annulla modulo p il discriminante della (7)] essa ha la radice doppia $\alpha \equiv -b(a^2 + 12b)/2a^3 - 8ab + 9b^2)$ e ammette due altre radici semplici per $\left(\frac{2b\alpha}{p}\right) = 1$.

4. Abbiamo poi preso ad applicare il procedimento generale del n. 1 alla congruenza (7) [senza passare, come indica la via classica, attraverso la sua risolvente cubica]. Si trova:

a) La congruenza

$$x^4 + ax^2 + bx + b \equiv 0 \pmod{p} \tag{7}$$

ha quattro radici incongrue quando i coefficienti a, b soddisfino le relazioni:

$$\begin{gathered} Q_{p-2}(a, b) \equiv 0, \quad Q_{p-3}(a, b) \equiv 0, \quad Q_{p-4}(a, b) \equiv 0; \\ b\,Q_{p-5}(a, b) \equiv (-1)^{\frac{p(p-1)}{2}+1} \end{gathered} \pmod{p} \tag{8}$$

essendo i polinomi $Q_h(a, b)$ definiti dalle relazioni:

$$\begin{aligned} Q_{2k}(a, b) &= \sum_{i,J} (-1)^i \binom{J}{2(J-i)} \binom{k-i}{J} a^{k-i-J} b^J \\ Q_{2k+1}(a, b) &= \sum_{i,J} (-1)^i \binom{J+1}{2(J-i)+1} \binom{k-i}{J+1} a^{k-i-J-1} b^{J+1} \end{aligned} \qquad k = 1, 2, \ldots \tag{9}$$

con le due somme estese a tutti i numeri interi non negativi i, J per i quali i termini dei coefficienti binomiali risultino non negativi e i numeratori maggiori o uguali ai denominatori, e al solito $\binom{a}{o} = 1$.

b) Data la congruenza (7) e supposto che essa abbia 4 radici, che siano cioè verificate le (8), il polinomio

$$2aQ_{\frac{p-5}{2}}(a, b) + 3b(-1)^{\frac{p-1}{2}} Q_{\frac{p-7}{2}}(a, b) - 4bQ_{\frac{p-9}{2}}$$

è, rispetto al modulo p, congruo con uno dei tre numeri

$$4\varepsilon, \quad 2\varepsilon, \quad 0$$

con $\varepsilon = \pm 1$, e nel primo caso la (7) ha 4 radici con lo stesso carattere quadratico modulo p, nel secondo una con carattere opposto alle altre tre, nel terzo due con lo stesso carattere quadratico e due con carattere quadratico opposto.

c) Conformemente alla teoria generale nel secondo caso (una radice con carattere quadratico opposto alle altre tre) la formula

$$x \equiv (-1)^{\frac{p-1}{2}} Q_{\frac{p-5}{2}}(a, b) / Q_{\frac{p-7}{2}}(a, b) \pmod{p}$$

dà la radice della (7) che non ha il carattere quadratico delle altre tre, nel terzo caso (due radici con lo stesso carattere quadratico e due con carattere quadratico opposto) si ha il resultato notevole: la formula

$$y \equiv 2(-1)^{\frac{p-1}{2}} b Q_{\frac{p-7}{2}}(a, b) / Q_{\frac{p-5}{2}}(a, b) \pmod{p}$$

fornisce una radice della risolvente cubica (di EULERO)

$$y^3 + 8ay^2 + (16a^2 - 64b)y - 64b^2 \equiv 0 \pmod{p}$$

della congruenza (7).

5. Per ultimo si studiano le congruenze

(7) $$x^4 + ax^2 + bx + b \equiv 0 \pmod{p}$$

prive di radici multiple, con un numero di radici minore del grado dell'equazione. Applicando la teoria del n. 1 si trova:

a) Data la congruenza (7) priva di radici multiple, si formi la matrice aritmetica [1]

$$\begin{array}{llll}
Q_{p-4} & Q_{p-3} & bQ_{p-5}+bQ_{p-6} & bQ_{p-5}+(-1)^{\frac{p(p-} \\
-Q_{p-3} & Q_{p-2} & bQ_{p-4}-bQ_{p-5}-(-1)^{\frac{p(p-1)}{2}} Q_{p-4} & \\
Q_{p-2} & Q_{p-1}-(-1)^{\frac{p(p-1)}{2}} & bQ_{p-3}+bQ_{p-4} & bQ_{p-3} \\
-Q_{p-1}+(-1)^{\frac{p(p-1)}{2}} & Q_p & bQ_{p-2}-bQ_{p-3} & bQ_{p-2}
\end{array}$$

[1] Nella matrice seguente, dappertutto dove è scritto Q, si legga $Q(a, b)$; l'abbreviazione è resa necessaria dall'esigenza dello spazio.

dove i polinomi $Q_h(a,b)$ hanno gli sviluppi dati dalle formule (9). Secondo che la matrice M modulo p ha la caratteristica 4, 3, 2, o la congruenza (7) è rispettivamente impossibile, oppure ha 1, 2, 4 radici.

b) Se M ha la caratteristica 3 modulo p, la radice della (1) è espressa dalla formula

$$x \equiv A_{4,3}/A_{44} \pmod{p}$$

dove $A_{4,3}$, A_{44} sono i complementi algebrici nel determinante M degli elementi della quarta riga posti rispettivamente nella terza e quarta colonna.

c) Se la matrice M ha la caratteristica 2 modulo p, le due radici della (7) soddisfano la congruenza di secondo grado

$$\begin{vmatrix} Q_{p-4} & Q_{p-3} \\ -Q_{p-3} & Q_{p-2} \end{vmatrix} x^2 + \begin{matrix} Q_{p-4} & bQ_{p+5} + bQ_{p-5} \\ -Q_{p-3} & bQ_{p-4} - bQ_{p-5} - (-1)^{\frac{p(p-1)}{2}} \end{matrix} \Bigg| x +$$

$$+ \begin{vmatrix} Q_{p-4} & bQ_{p-5} + (1-)^{\frac{p(p-1)}{2}} \\ -Q_{p-3} & bQ_{p-4} \end{vmatrix} \equiv 0 \pmod{p}$$

risolubile con l'ordinaria formula dell'algebra, estraendo le radici quadrate con la formula di CIPOLLA.

Firenze, aprile 1928.